IBM Security QRadar

バージョン 7.3.0

管理ガイド

注記

本書および本書で紹介する製品をご使用になる前に、 479 ページの『特記事項』に記載されている情報をお読みください。

この資料は、IBM QRadar Security Intelligence Platform V7.3.0 に適用されます。また、この資料の更新版が公開されない限り、これ以降のリリースにも適用されます。

お客様の環境によっては、資料中の円記号がバックスラッシュと表示されたり、バックスラッシュが円記号と表示されたりする場合があります。

原典： IBM Security QRadar
Version 7.3.0
Administration Guide

発行： 日本アイ・ビー・エム株式会社

担当： トランスレーション・サービス・センター

目次

QRadar 製品管理の概要

管理者は、IBM® Security QRadar® SIEM を使用して、ダッシュボード、オフェンス、ログ・アクティビティー、ネットワーク・アクティビティー、アセット、およびレポートを管理することができます。

対象読者

このガイドは、ネットワーク・セキュリティーの調査と管理を担当するすべての QRadar SIEM ユーザーを対象としています。このガイドは、QRadar SIEM へのアクセス権限とご使用の企業ネットワークとネットワーキング・テクノロジーに関する知識をお持ちの方を想定して記述されています。

技術資料

IBM Security QRadar の製品資料 (すべての翻訳資料を含む) を Web 上で探すには、IBM Knowledge Center (http://www.ibm.com/support/knowledgecenter/SS42VS/welcome) にアクセスしてください。

QRadar 製品ライブラリーでより技術的な資料にアクセスする方法については、Accessing IBM Security Documentation Technical Note (www.ibm.com/support/docview.wss?rs=0&uid=swg21614644) を参照してください。

お客様サポートへの連絡

お客様サポートへのお問い合わせについては、Support for IBM Security QRadar (http://www.ibm.com/support/docview.wss?rs=0&uid=swg21612861) を参照してください。

適切なセキュリティーの実践に関する注意事項

IT システムのセキュリティーでは、企業の内部と外部からの不正なアクセスの防止、検出、対応により、システムと情報を保護する必要があります。不正なアクセスにより、情報の改ざん、破壊、盗用、悪用が発生したり、使用しているシステムの損傷や、他のシステムに対する攻撃のための利用を含む悪用につながる可能性があります。完全に安全と見なすことができる IT システムまたは IT 製品は存在せず、また単一の製品、サービス、またはセキュリティー対策が、不適切な使用またはアクセスを防止する上で、完全に有効となることもありません。IBM のシステム、製品およびサービスは、合法かつ包括的なセキュリティーの取り組みの一部となるように設計されており、これらには必ず追加の運用手順が伴います。また、最高の効果を得るために、他のシステム、製品、またはサービスを必要とする場合があります。IBM は、何者かの悪意のある行為または違法行為によって、システム、製品、またはサービスのいずれも影響を受けないこと、またはお客様の企業がそれらの行為によって影響を受けないことを保証するものではありません。

注意:

本プログラムの利用は、様々な法律または規制に関わる場合があります。これには、プライバシー、データ保護、雇用、電子通信、および電子保管に関連するもの

が含まれます。IBM Security QRadar は、合法的な目的のために合法的な手段を用いてのみ使用することができます。お客様は、適用される法律、規制、およびポリシーに従って本プログラムを使用することに同意し、かかる法律、規制、およびポリシーを遵守する全責任を負うものとします。ライセンシーは、IBM Security QRadar の合法的な使用に必要なすべての同意、許可、または使用権を取得するか、取得済みであることを表明するものとします。

第 1 章 QRadar V7.3.0 の管理に関する新機能

IBM Security QRadar V7.3.0 では、テナント・ユーザー向けの新機能、改善されたセキュリティー、柔軟性が向上したライセンス管理、アプリケーション共有のための専用アプリケーション・ノードが導入されています。

強固なパスワードによる QRadar インスタンスの保護

QRadar V7.3.0.2 では、強固なパスワード・ポリシーが導入されています。ポリシーを有効にする場合、システム認証パスワードには最小文字数が含まれている必要があり、またオプションで、大文字、小文字、特殊文字、数字の各属性のうち少なくとも 3 つの属性が含まれている必要があります。要件を満たさないパスワードでログインするユーザーに対しては、パスワードの変更を求めるプロンプトが出されます。

パスワード・ポリシー設定は、QRadar によって管理される (システム認証) 管理ユーザー・パスワードおよび非管理ユーザー・パスワードに適用され、別の認証プロバイダーによって管理される (外部認証) パスワード、およびルート・パスワードには適用されません。

 システム認証の構成に関する詳細...

ログ・ソース制限の除去

QRadar V7.3.0 でのライセンス交付モデルの改善により、ログ・ソースの管理がより簡単になりました。ログ・ソース制限が除去され、ログ・ソース用にライセンスを購入する必要はなくなりました。

QRadar V7.3.0 にアップグレードすると、以前のログ・ソース制限は除去されます。

デプロイメント環境全体へのイベントおよびフローのキャパシティーの容易な分散

ライセンスが割り振られているホストに関係なく、デプロイメント環境内の任意のホストに 1 秒当たりのイベント数 (EPS) と 1 分当たりのフロー数 (FPM) を割り振ることによって、ワークロードの変化に対応します。

個々のライセンスの EPS および FPM は、共有ライセンス・プールに集約されるようになりました。管理者は、新しい「ライセンス・プール管理」ウィンドウを使用して、デプロイメント環境全体の累積の EPS および FPM のキャパシティーを素早く確認し、管理対象ホストに EPS と FPM を割り振る最善の方法を決定できます。

例えば、QRadar V7.2.8 分散デプロイメント環境に 2 つのイベント・プロセッサーがあり、それぞれ 7,500 EPS と 15,000 EPS が割り振られているとします。QRadar V7.3.0 にアップグレードすると、各プロセッサーはアップグレード前の EPS 割り振りを維持しますが、合計された 22,500 EPS が共有ライセンス・プール

の一部となります。イベント・プロセッサーのデータ・ボリュームが変化したり、管理対象ホストを追加したりした場合、EPS 容量を再配分できます。

 共有ライセンス・プールの管理に関する詳細...

テナント・ユーザーによるカスタム・プロパティーの作成が可能

テナント・ユーザーは、カスタム・プロパティーを作成することで、マネージド・セキュリティー・サービス・プロバイダー (MSSP) 管理者の支援なしに、イベント・ペイロードまたはフロー・ペイロードから重要な情報を抽出したり計算したりできます。この機能を使用すると、テナント・ユーザーは、QRadar が通常は正規化したり表示したりしないようなデータを表示および検索できます。

MSSP 管理者は、テナント・ユーザーが作成したすべてのカスタム・プロパティーに対する書き込み権限を持っています。ルールおよびレポートでテナントのカスタム・プロパティーが頻繁に使用される場合、管理者は、検索のパフォーマンスを向上させるために、このプロパティーを最適化できます。テナント・ユーザーは、自身が作成したプロパティーを最適化することはできません。

カスタム・イベント・プロパティーとカスタム・フロー・プロパティーの操作方法について詳しくは、「*IBM Security QRadar* ユーザー・ガイド」を参照してください。

テナント・ユーザーによるリファレンス・データ収集の作成が可能

QRadar V7.2.8 では、テナント・ユーザーは、MSSP 管理者によって作成されたリファレンス・データを表示できます。V7.3.0 では、「代行管理」 > 「リファレンス・データの管理」ユーザー・ロールを持つテナント・ユーザーは、MSSP 管理者の支援なしに、独自のリファレンス・データ収集を作成および管理できるようになりました。

この機能を使用すると、テナント・ユーザーは、参照用のビジネス・データや外部ソースからのデータを追跡し、それを QRadar の検索、フィルター、ルール・テスト条件、およびルール応答で使用できます。例えば、解雇された従業員のユーザー ID を含むリファレンス・セットを使用して、従業員がネットワークにログインするのを防ぐことができます。

 リファレンス・データ収集の作成方法および管理方法の詳細...

専用アプリケーション・ノードからの QRadar アプリケーションのサービス提供

QRadar V7.3.0 より前では、すべての QRadar アプリケーションは QRadar コンソールにインストールする必要がありました。多数のアプリケーションがインストールされているシステムや、リソースを多く使用するアプリケーションがインストールされているシステムでは、QRadar コンソールのメモリー、ストレージ、および CPU リソースの制限のため、パフォーマンスの問題が発生する可能性があります。

QRadar V7.3.0 では、QRadar コンソールにインストールされているアプリケーションのパフォーマンスを制限することなくアプリケーションおよびアプリケーション・データを処理する、専用のアプリケーション・ノード・サーバーをインストールできるようになりました。

必要なメモリー、ストレージ、および CPU リソースを備えた Red Hat Enterprise Linux 7.2 サーバーまたは CentOS 7.2 サーバーをセットアップする際に、QRadar の「管理」タブからアプリケーション・ノードを数分でインストールできます。アプリケーション・ノードのインストール・プロセスでは、すべての必要なソフトウェアがインストールされ、QRadar コンソールにインストールされたすべてのアプリケーションがアプリケーション・ノードに転送されます。

 アプリケーション・ノードのセットアップに関する詳細...

アプリケーションのバックアップおよびリカバリーのプロセスの最適化

アプリケーションの構成をバックアップし、アプリケーション・データとは別にリストアできるようになりました。

アプリケーションの構成は、毎晩の構成バックアップの一環としてバックアップされます。構成バックアップには、QRadar コンソールにインストールされたアプリケーションと、アプリケーション・ノードにインストールされたアプリケーションが含まれます。バックアップのリストア時に「インストール済みアプリケーションの構成」オプションを選択することにより、アプリケーションの構成をリストアできます。

アプリケーション・データは、使いやすいスクリプトを使用して、アプリケーションの構成とは別にバックアップされます。このスクリプトは毎晩実行されます。また、このスクリプトを使用して、アプリケーション・データをリストアしたり、バックアップ時間およびデータ保存期間を構成したりすることもできます。

 アプリケーションのバックアップおよびリストアに関する詳細...

 アプリケーション・データのバックアップおよびリストアに関する詳細...

セキュリティーの更新

QRadar V7.3.0 は、セキュアな通信のために TLS 1.2 (Transport Layer Security) を使用します。Secure Socket Layer (SSL) および TLS 1.1 プロトコルはサポートされません。

プロキシー・サーバー経由の自動更新では、デフォルト CA 証明書の更新手順に多少の変更があります。

第 2 章 QRadar 管理の概要

IBM Security QRadar 管理者が QRadar デプロイメント環境の構成と管理を行う際に役立つ各種のツールが用意されています。

例えば、「管理」タブにあるツールを使用して、以下の作業を実行できます。

- QRadar のホストおよびライセンスのデプロイと管理を行う。
- ユーザー・アカウントおよびユーザー認証を構成する。
- ネットワーク階層を構築する。
- ドメインを構成し、マルチテナント環境をセットアップする。
- ログ・ソースおよびフロー・データ・ソースを定義および管理する。
- QRadar のデータ保存を管理する。
- アセットおよびリファレンス・データを管理する。
- QRadar の構成およびデータの定期的なバックアップをスケジュールする。
- 管理対象ホストのシステム・ヘルスをモニターする。

IBM Security QRadar 製品の機能

IBM Security QRadar 製品資料では、オフェンス、フロー、アセット、ヒストリカル相関などの機能について説明していますが、すべての QRadar 製品でこれらの機能を利用できるわけではありません。使用する製品によっては、説明されている一部の機能をデプロイメントで使用できない場合があります。各製品の機能を確認して、必要な情報を入手してください。

IBM QRadar Log Manager

QRadar Log Manager は、ネットワークおよびセキュリティーの大量のイベント・ログを収集、分析、保管、およびレポートするための基本的なハイパフォーマンスかつスケーラブルなソリューションです。

IBM Security QRadar SIEM

QRadar SIEM は、オンプレミスのデプロイメント用のあらゆる種類のセキュリティー・インテリジェンス機能を含む、拡張オファリングです。ネットワーク上に分散している数千にのぼるアセット、デバイス、エンドポイント、およびアプリケーションからのログ・ソースとネットワーク・フロー・データを統合し、生データに対して正規化および相関アクティビティーを即時に実行して、実際に発生している脅威とフォールス・ポジティブを区別します。

IBM QRadar on Cloud

QRadar on Cloud では、IBM のセキュリティー専門家がインフラストラクチャーを管理する一方で、お客様のセキュリティー・アナリストが脅威の検出と管理の作業を実行します。総所有コストを削減しながら、ネットワークを保護し、コンプライアンスの監視と報告の要件を満たすことができます。

QRadar 製品の機能

IBM Security QRadar 製品資料では、オフェンス、フロー、アセット、ヒストリカル相関などの機能について説明していますが、すべての QRadar 製品でこれらの機能を利用できるわけではありません。各製品の機能比較については、以下の表を確認してください。

表 *1. QRadar* の機能の比較

機能	**QRadar SIEM**	**IBM QRadar on Cloud**	**IBM QRadar Log Manager**
全管理機能	はい	いいえ	はい
ホスト・デプロイメントのサポート	いいえ	はい	いいえ
カスタマイズ可能なダッシュボード	はい	はい	はい
カスタム・ルール・エンジン	はい	はい	はい
ネットワーク・イベントおよびセキュリティー・イベントの管理	はい	はい	はい
ホストおよびアプリケーションのログの管理	はい	はい	はい
しきい値ベースのアラート	はい	はい	はい
コンプライアンス・テンプレート	はい	はい	はい
データ・アーカイブ	はい	はい	はい
IBM Security X-Force® Threat Intelligence IP レピュテーション・フィードの統合	はい	はい	はい
WinCollect スタンドアロン・デプロイメント	はい	はい	はい
WinCollect 管理デプロイメント	はい	いいえ	はい
QRadar Vulnerability Manager の統合	はい	はい	はい
ネットワーク・アクティビティー・モニタリング	はい	はい	いいえ
アセット・プロファイル	はい	はい	いいえ [1]
オフェンス管理	はい	はい	いいえ
ネットワーク・フローのキャプチャーと分析	はい	いいえ	いいえ
ヒストリカル相関	はい	はい	いいえ
QRadar Risk Manager の統合	はい	いいえ	いいえ
QRadar Incident Forensics の統合	はい	いいえ	いいえ
[1] QRadar Vulnerability Manager がインストールされている場合に限り、QRadar Log Manager はアセット・データを追跡します。			

「管理ガイド」や「ユーザーズ・ガイド」などの一部の資料は複数の製品間で共通であり、ご使用のデプロイメント環境では使用できない機能が説明されている場合があります。例えば、IBM QRadar on Cloud のユーザーは、「*IBM Security QRadar* 管理ガイド」に説明されている完全な管理機能は使用できません。

関連概念:

241 ページの『第 14 章 リモート・ネットワークおよびサービスの構成』
リモート・ネットワーク・グループとサービス・グループを使用して、ネットワーク上の特定のプロファイル用のトラフィック・アクティビティーを表します。リモート・ネットワーク・グループには、指定されたリモート・ネットワークから発生するユーザー・トラフィックが表示されます。

サポート対象の Web ブラウザー

IBM Security QRadar 製品の機能が正しく動作するためには、サポート対象の Web ブラウザーを使用する必要があります。

以下の表に、サポートされる Web ブラウザーのバージョンをリストします。

表 2. *QRadar* 製品でサポートされる *Web* ブラウザー

Web ブラウザー	サポート対象のバージョン
Mozilla Firefox	45.2 延長サポート版
64 ビット版の Microsoft Internet Explorer (Microsoft Edge モードを有効にすること)。	11.0
Google Chrome	54 および 55

第 3 章 ユーザー管理

ユーザー・ロール、セキュリティー・プロファイル、およびユーザー・アカウントを定義して、どのユーザーが IBM Security QRadar にアクセスできるか、どのタスクをそのユーザーが実行できるか、およびどのデータにそのユーザーがアクセスできるかを制御します。

IBM Security QRadar の「管理」タブにある「ユーザー管理」機能を使用して、ユーザー・アカウントの構成と管理を行います。

QRadar を初めて構成する場合は、QRadar にアクセスする必要があるすべてのユーザーについて、ユーザー・アカウントを作成してください。

関連概念:

5 ページの『IBM Security QRadar 製品の機能』
IBM Security QRadar 製品資料では、オフェンス、フロー、アセット、ヒストリカル相関などの機能について説明していますが、すべての QRadar 製品でこれらの機能を利用できるわけではありません。使用する製品によっては、説明されている一部の機能をデプロイメントで使用できない場合があります。各製品の機能を確認して、必要な情報を入手してください。

ユーザー・ロール

ユーザー・ロールは、ユーザーが IBM Security QRadar でアクセスできる機能を定義します。

インストール時に、「管理」と「すべて」という 2 つのデフォルトのユーザー・ロールが定義されます。

ユーザー・アカウントを追加する前に、ユーザーの権限要件を満たすためにユーザー・ロールを作成する必要があります。

ユーザー・ロールの作成

ユーザー・ロールを作成し、ユーザーが IBM Security QRadar でアクセスできる機能を管理します。

このタスクについて

デフォルトでは、ご使用のシステムには、デフォルトの管理ユーザー・ロール (QRadar のすべての領域にアクセスできるロール) が用意されています。管理ユーザー・ロールが割り当てられたユーザーは、自分のアカウントを編集することはできません。この制限は、デフォルトの「管理」ユーザー・ロールにも適用されます。アカウントの変更は、別の管理ユーザーが行う必要があります。

手順

1. 「管理」タブをクリックします。

2. ナビゲーション・メニューで、「システム構成」 > 「ユーザー管理」をクリックします。
3. 「ユーザー・ロール」アイコンをクリックします。
4. ツールバーで、「新規」をクリックします。
5. 「ユーザー・ロール名 **(User Role Name)**」フィールドに、このユーザー・ロールの固有名を入力します。
6. このユーザー・ロールに割り当てる権限を選択します。

   ユーザー・ロール権限に関する詳細の説明**:**

   「ユーザー・ロール管理」ウィンドウに表示される権限は、インストールされている QRadar コンポーネントによって異なります。

表 *3.* 「ユーザー・ロール管理」ウィンドウの権限の説明

権限	説明
管理	ユーザー・インターフェースへの管理アクセス権限を付与します。特定の管理権限を付与できます。 「システム管理者」権限を持つユーザーは、ユーザー・インターフェースの全領域にアクセスできます。このアクセス権限を持つユーザーは、他の管理者アカウントを編集できません。
代行管理	限定的な管理機能を実行する権限をユーザーに付与します。複数テナント環境では、「代行管理」権限があるテナント・ユーザーは、自分のテナント環境のデータのみを表示できます。「代行管理」に属さない他の管理権限を割り当てると、テナント・ユーザーは、すべてのテナントのデータを表示できます。
オフェンス	「オフェンス」タブのすべての機能に対するアクセス権限を付与します。 カスタム・ルールを作成および編集するには、ユーザー・ロールに「カスタム・ルールの保守」権限が必要です。

表 3. 「ユーザー・ロール管理」ウィンドウの権限の説明 (続き)

権限	説明
ログ・アクティビティー	「ログ・アクティビティー」タブの各機能に対するアクセス権限を付与します。以下に示す特定の権限を付与することもできます。 カスタム・ルールの保守 「ログ・アクティビティー」タブに表示されるルールを作成および編集するための権限を付与します。 時系列の管理 時系列データ・グラフを構成および表示するための権限を付与します。 ユーザー定義のイベント・プロパティー カスタム・イベント・プロパティーを作成するための権限を付与します。 カスタム・ルールの表示 カスタム・ルールを表示するための権限を付与します。「カスタム・ルールの保守」権限も同時に保持していないユーザー・ロールにこの権限を付与すると、そのユーザー・ロールはカスタム・ルールを作成および編集できません。
アセット	**注:** この権限は、IBM Security QRadar Vulnerability Manager がシステムにインストールされている場合のみ表示されます。 「アセット」タブの各機能に対するアクセス権限を付与します。以下に示す特定の権限を付与できます。 **VA** スキャンの実行 **(Perform VA Scans)** 脆弱性評価スキャンを実行するための権限を付与します。脆弱性評価について詳しくは、「*Managing Vulnerability Assessment Guide*」を参照してください。 脆弱性の除去 **(Remove Vulnerabilities)** アセットから脆弱性を除去するための権限を付与します。 サーバー・ディスカバリー サーバーをディスカバーするための権限を付与します。 **VA** データの表示 **(View VA Data)** 脆弱性評価のデータに対するアクセス権を付与します。脆弱性評価について詳しくは、「*Managing Vulnerability Assessment*」ガイドを参照してください。

表 3. 「ユーザー・ロール管理」ウィンドウの権限の説明 (続き)

権限	説明
ネットワーク・アクティビティー	「ネットワーク・アクティビティー」タブのすべての機能に対するアクセス権限を付与します。以下に示す権限に対する特定のアクセス権限を付与できます。 カスタム・ルールの保守 「ネットワーク・アクティビティー」タブに表示されるルールを作成および編集するための権限を付与します。 時系列の管理 時系列データ・グラフを構成および表示するための権限を付与します。 ユーザー定義のフロー・プロパティー カスタム・フロー・プロパティーを作成するための権限を付与します。 カスタム・ルールの表示 カスタム・ルールを表示するための権限を付与します。ユーザー・ロールが「カスタム・ルールの保守」権限も同時に保持していない場合、そのユーザー・ロールはカスタム・ルールを作成および編集できません。 フロー・コンテンツの表示 フロー・データにアクセスするための権限を付与します。
レポート	「レポート」タブのすべての機能にアクセスするための権限を付与します。 **E** メール経由でレポートを配布 E メール経由でレポートを配布するための権限を付与します。 テンプレートの保守 レポート・テンプレートを編集するための権限を付与します。
Vulnerability Manager	QRadar Vulnerability Manager の機能に対するアクセス権を付与します。QRadar Vulnerability Manager がアクティブ化されている必要があります。 詳しくは、「*IBM Security QRadar Vulnerability Manager* ユーザー・ガイド」を参照してください。
Forensics	QRadar Incident Forensics の機能に対するアクセス権を付与します。 **Incident Forensics** でケースを作成 **(Create cases in Incident Forensics)** インポートされた文書および PCAP ファイルの収集に関するケースを作成する権限を付与します。
IP 右クリックメニュー拡張	右クリック・メニューに追加されるオプションに対するアクセス権を付与します。

表 3. 「ユーザー・ロール管理」ウィンドウの権限の説明 (続き)

権限	説明
プラットフォームの構成	「プラットフォームの構成」のサービスに対するアクセス権を付与します。 システム通知の解除 **(Dismiss System Notifications)** 「メッセージ」タブにシステム通知が表示されないようにするための権限を付与します。 リファレンス・データの表示 **(View Reference Data)** 検索結果内のリファレンス・データを表示するための権限を付与します。 システム通知の表示 **(View System Notifications)** 「メッセージ」タブにシステム通知を表示するための権限を付与します。

7. 「ダッシュボード」領域で、ユーザー・ロールにアクセス権限を付与するダッシュボードを選択し、「追加」をクリックします。

   注**:** ユーザー・ロールにダッシュボード・データを表示するための権限がない場合、そのダッシュボードには情報が表示されません。ユーザーが表示されたダッシュボードを変更すると、そのユーザー・ロールに対して定義されたダッシュボードが、次回のログイン時に表示されます。
8. 「保存」をクリックして「ユーザー・ロール管理」ウィンドウを閉じます。
9. 「管理」タブ・メニューで、「変更のデプロイ」をクリックします。

ユーザー・ロールの編集

既存のロールを編集して、そのロールに割り当てる権限を変更することができます。

このタスクについて

編集するユーザー・ロールを「ユーザー・ロール管理」ウィンドウで素早く見つけるには、「入力してフィルタリング」テキスト・ボックスにロール名を入力します。このボックスは、左ペインの上にあります。

手順

1. 「管理」タブをクリックします。
2. ナビゲーション・メニューで、「システム構成」 > 「ユーザー管理」をクリックします。
3. 「ユーザー・ロール」アイコンをクリックします。
4. 「ユーザー・ロール管理 (User Role Management)」ウィンドウの左ペインで、編集するユーザー・ロールを選択します。
5. 必要に応じて、右ペインで権限を更新します。

   ユーザー・ロール権限に関する詳細の説明**:**

   「ユーザー・ロール管理」ウィンドウに表示される権限は、インストールされている QRadar コンポーネントによって異なります。

表 4. 「ユーザー・ロール管理」ウィンドウの権限の説明

権限	説明
管理	ユーザー・インターフェースへの管理アクセス権限を付与します。特定の管理権限を付与できます。 「システム管理者」権限を持つユーザーは、ユーザー・インターフェースの全領域にアクセスできます。このアクセス権限を持つユーザーは、他の管理者アカウントを編集できません。
代行管理	限定的な管理機能を実行する権限をユーザーに付与します。複数テナント環境では、「代行管理」権限があるテナント・ユーザーは、自分のテナント環境のデータのみを表示できます。「代行管理」に属さない他の管理権限を割り当てると、テナント・ユーザーは、すべてのテナントのデータを表示できます。
オフェンス	「オフェンス」タブのすべての機能に対するアクセス権限を付与します。 カスタム・ルールを作成および編集するには、ユーザー・ロールに「カスタム・ルールの保守」権限が必要です。
ログ・アクティビティー	「ログ・アクティビティー」タブの各機能に対するアクセス権限を付与します。以下に示す特定の権限を付与することもできます。 カスタム・ルールの保守 「ログ・アクティビティー」タブに表示されるルールを作成および編集するための権限を付与します。 時系列の管理 時系列データ・グラフを構成および表示するための権限を付与します。 ユーザー定義のイベント・プロパティー カスタム・イベント・プロパティーを作成するための権限を付与します。 カスタム・ルールの表示 カスタム・ルールを表示するための権限を付与します。「カスタム・ルールの保守」権限も同時に保持していないユーザー・ロールにこの権限を付与すると、そのユーザー・ロールはカスタム・ルールを作成および編集できません。

表 4. 「ユーザー・ロール管理」ウィンドウの権限の説明 (続き)

権限	説明
アセット	**注:** この権限は、IBM Security QRadar Vulnerability Manager がシステムにインストールされている場合のみ表示されます。 「アセット」タブの各機能に対するアクセス権限を付与します。以下に示す特定の権限を付与できます。 **VA** スキャンの実行 **(Perform VA Scans)** 脆弱性評価スキャンを実行するための権限を付与します。脆弱性評価について詳しくは、「*Managing Vulnerability Assessment Guide*」を参照してください。 脆弱性の除去 **(Remove Vulnerabilities)** アセットから脆弱性を除去するための権限を付与します。 サーバー・ディスカバリー サーバーをディスカバーするための権限を付与します。 **VA** データの表示 **(View VA Data)** 脆弱性評価のデータに対するアクセス権を付与します。脆弱性評価について詳しくは、「*Managing Vulnerability Assessment*」ガイドを参照してください。
ネットワーク・アクティビティー	「ネットワーク・アクティビティー」タブのすべての機能に対するアクセス権限を付与します。以下に示す権限に対する特定のアクセス権限を付与できます。 カスタム・ルールの保守 「ネットワーク・アクティビティー」タブに表示されるルールを作成および編集するための権限を付与します。 時系列の管理 時系列データ・グラフを構成および表示するための権限を付与します。 ユーザー定義のフロー・プロパティー カスタム・フロー・プロパティーを作成するための権限を付与します。 カスタム・ルールの表示 カスタム・ルールを表示するための権限を付与します。ユーザー・ロールが「カスタム・ルールの保守」権限も同時に保持していない場合、そのユーザー・ロールはカスタム・ルールを作成および編集できません。 フロー・コンテンツの表示 フロー・データにアクセスするための権限を付与します。

表 4. 「ユーザー・ロール管理」ウィンドウの権限の説明 (続き)

権限	説明
レポート	「レポート」タブのすべての機能にアクセスするための権限を付与します。 **E** メール経由でレポートを配布 E メール経由でレポートを配布するための権限を付与します。 テンプレートの保守 レポート・テンプレートを編集するための権限を付与します。
Vulnerability Manager	QRadar Vulnerability Manager の機能に対するアクセス権を付与します。QRadar Vulnerability Manager がアクティブ化されている必要があります。 詳しくは、「*IBM Security QRadar Vulnerability Manager* ユーザー・ガイド」を参照してください。
Forensics	QRadar Incident Forensics の機能に対するアクセス権を付与します。 **Incident Forensics** でケースを作成 **(Create cases in Incident Forensics)** インポートされた文書および PCAP ファイルの収集に関するケースを作成する権限を付与します。
IP 右クリックメニュー拡張	右クリック・メニューに追加されるオプションに対するアクセス権を付与します。
プラットフォームの構成	「プラットフォームの構成」のサービスに対するアクセス権を付与します。 システム通知の解除 **(Dismiss System Notifications)** 「メッセージ」タブにシステム通知が表示されないようにするための権限を付与します。 リファレンス・データの表示 **(View Reference Data)** 検索結果内のリファレンス・データを表示するための権限を付与します。 システム通知の表示 **(View System Notifications)** 「メッセージ」タブにシステム通知を表示するための権限を付与します。

6. 必要に応じて、ユーザー・ロールの「ダッシュボード」のオプションを変更します。
7. 「保存」をクリックします。
8. 「ユーザー・ロール管理」ウィンドウを閉じます。
9. 「管理」タブ・メニューで、「変更のデプロイ」をクリックします。

ユーザー・ロールの削除

ユーザー・ロールが不要になった場合は、そのユーザー・ロールを削除してかまいません。

このタスクについて

削除したいユーザー・ロールにユーザー・アカウントが割り当てられている場合は、そのユーザー・アカウントを別のユーザー・ロールに再割り当てする必要があります。システムは、この状況を自動的に検出して、ユーザー・アカウントを更新するためのプロンプトを表示します。

削除対象のユーザー・ロールは、「ユーザー・ロール管理」ウィンドウですぐに見つけることができます。左ペインの上にある「入力してフィルタリング」テキスト・ボックスに、ロール名を入力します。

手順

1. 「管理」タブをクリックします。
2. ナビゲーション・メニューで、「システム構成」 > 「ユーザー管理」をクリックします。
3. 「ユーザー・ロール」アイコンをクリックします。
4. 「ユーザー・ロール管理 (User Role Management)」ウィンドウの左ペインで、削除するロールを選択します。
5. ツールバーで、「削除」をクリックします。
6. 「**OK**」をクリックします。
   - このユーザー・ロールにユーザー・アカウントが割り当てられている場合は、「ユーザーがこのユーザー・ロールに割り当てられています (Users are Assigned to this User Role)」ウィンドウが開きます。ステップ 7 に進みます。
   - このロールにユーザー・アカウントが割り当てられていない場合は、ユーザー・ロールが正常に削除されます。その場合は、ステップ 8 に進みます。
7. リストされているユーザー・アカウントを別のユーザー・ロールに再割り当てします。
   a. 「割り当てるユーザー・ロール **(User Role to assign)**」リスト・ボックスから、ユーザー・ロールを選択します。
   b. 「確認 **(Confirm)**」をクリックします。
8. 「ユーザー・ロール管理」ウィンドウを閉じます。
9. 「管理」タブ・メニューで、「変更のデプロイ」をクリックします。

セキュリティー・プロファイル

セキュリティー・プロファイルは、ユーザーがアクセスできるネットワーク、ログ・ソース、およびドメインを定義します。

QRadar には、管理ユーザー用のデフォルトのセキュリティー・プロファイルが 1 つ用意されています。「管理」セキュリティー・プロファイルには、すべてのネットワーク、ログ・ソース、およびドメインに対するアクセス権限が含まれています。

ユーザー・アカウントを追加する前に、ユーザーの特定のアクセス要件を満たすために、追加のセキュリティー・プロファイルを作成する必要があります。

ドメイン

セキュリティー・プロファイルを、関連付けたドメインで更新する必要があります。「ドメイン」タブが「セキュリティー・プロファイル管理」ウィンドウに表示される前に、「ドメイン管理」ウィンドウでドメインを定義する必要があります。ドメイン・レベルの制限は、セキュリティー・プロファイルが更新されて変更がデプロイされるまで適用されません。

ドメインの割り当ては、「許可の優先順位」タブ、「ネットワーク」タブ、および「ログ・ソース」タブのすべての設定よりも優先されます。

そのドメインがテナントに割り当てられている場合は、テナント名が、「割り当て済みのドメイン」ウィンドウのドメイン名の横に括弧付きで表示されます。

権限の優先順位

権限の優先順位により、システムが「ログ・アクティビティー」タブにイベントを表示し、「ネットワーク・アクティビティー」タブにフローを表示するときに考慮の対象となるセキュリティー・プロファイル・コンポーネントが決定されます。

セキュリティー・プロファイルを作成する際は、以下の制限から選択します。

- 制限なし - このオプションは、「ログ・アクティビティー」タブに表示されるイベントや、「ネットワーク・アクティビティー」タブに表示されるフローに対して、制限を適用しません。
- ネットワークのみ - このオプションは、このセキュリティー・プロファイルで指定されたネットワークに関連するイベントおよびフローだけを表示できるようにユーザーを制限します。
- ログ・ソースのみ - このオプションは、このセキュリティー・プロファイルで指定されたログ・ソースに関連するイベントだけを表示できるようにユーザーを制限します。
- ネットワークとログ・ソース **(Networks AND Log Sources)** - このオプションでは、ユーザーは、このセキュリティー・プロファイルで指定されたログ・ソースとネットワークに関連するイベントとフローだけを表示できます。

  例えば、セキュリティー・プロファイルによりログ・ソースからイベントへのアクセスが許可されているが、宛先ネットワークが制限されている場合、そのイベントは「ログ・アクティビティー」タブには表示されません。この場合、イベントは、両方の要件を満たしている必要があります。
- ネットワークまたはログ・ソース - このオプションでは、ユーザーは、このセキュリティー・プロファイルで指定されたログ・ソースまたはネットワークに関連するイベントおよびフローを表示できます。

例えば、セキュリティー・プロファイルによりログ・ソースからイベントへのアクセスが許可されているが、宛先ネットワークが制限されている場合、許可の優先順位が「ネットワークまたはログ・ソース」に設定されていれば、イベントは「ログ・アクティビティー」タブに表示されます。許可の優先順位が「ネットワークおよびログ・ソース」に設定されている場合、そのイベントは「ログ・アクティビティー」タブには表示されません。

オフェンス・データの権限の優先順位

オフェンス・データが表示されると、セキュリティー・プロファイルは自動的に「ネットワークまたはログ・ソース」権限を使用します。例えば、セキュリティー・プロファイルがユーザーに表示を許可している宛先 IP アドレスがオフェンスにあるが、セキュリティー・プロファイルが送信元 IP アドレスに権限を付与しない場合、「オフェンスのサマリー」ウィンドウに宛先 IP アドレスと送信元 IP アドレスの両方が表示されます。

セキュリティー・プロファイルの作成

ユーザー・アカウントを追加するには、ユーザーの特定のアクセス要件を満たすために、まずセキュリティー・プロファイルを作成する必要があります。

このタスクについて

IBM Security QRadar SIEM には、管理ユーザー用のデフォルトのセキュリティー・プロファイルが 1 つ用意されています。「管理」セキュリティー・プロファイルには、すべてのネットワーク、ログ・ソース、およびドメインに対するアクセス権限が含まれています。

「セキュリティー・プロファイル管理」ウィンドウで複数の項目を選択するには、Ctrl キーを押しながら、追加したいネットワークまたはネットワーク・グループを選択します。

ネットワーク、ログ・ソース、またはドメインを追加した後に、その 1 つ以上を削除してから構成を保存する場合は、項目を選択して「削除 **(<)**」アイコンをクリックします。すべての項目を削除するには、「すべて削除」をクリックします。

手順

1. 「管理」タブをクリックします。
2. ナビゲーション・メニューで、「システム構成」 > 「ユーザー管理」をクリックします。
3. 「セキュリティー・プロファイル **(Security Profiles)**」アイコンをクリックします。
4. 「セキュリティー・プロファイル管理」ウィンドウで、「新規」をクリックします。
5. 以下のパラメーターを構成します。
   a. 「セキュリティー・プロファイル名」フィールドに、セキュリティー・プロファイルの固有名を入力します。セキュリティー・プロファイル名は、以下の要件を満たしている必要があります。3 文字以上であること、30 文字以内であること。
   b. **オプション**: セキュリティー・プロファイルの説明を入力します。最大 255 文字まで入力できます。
6. 「権限の優先順位 **(Permission Precedence)**」タブをクリックします。
7. 「権限の優先順位の設定 (Permission Precedence Setting)」ペインで、権限の優先順位オプションを選択します。 18 ページの『権限の優先順位』を参照してください。

8. セキュリティー・プロファイルに割り当てるネットワークを構成します。
   a. 「ネットワーク **(Networks)**」タブをクリックします。
   b. 「ネットワーク **(Networks)**」タブの左ペインのナビゲーション・ツリーで、このセキュリティー・プロファイルがアクセスするネットワークを選択します。
   c. 「追加 **(Add) (>)**」アイコンをクリックして、ネットワークを「割り当てられたネットワーク (Assigned Networks)」ペインに追加します。
   d. 追加するネットワークごとに繰り返します。
9. セキュリティー・プロファイルに割り当てるログ・ソースを構成します。
   a. 「ログ・ソース」タブをクリックします。
   b. 左ペインのナビゲーション・ツリーで、このセキュリティー・プロファイルがアクセスするログ・ソース・グループまたはログ・ソースを選択します。
   c. 「追加 **(Add) (>)**」アイコンをクリックして、ログ・ソースを「割り当てられたログ・ソース (Assigned Log Sources)」ペインに追加します。
   d. 追加するログ・ソースごとに繰り返します。
10. セキュリティー・プロファイルに割り当てるドメインを以下の手順で構成します。
   a. 「ドメイン」タブをクリックします。
   b. 左ペインのナビゲーション・ツリーで、このセキュリティー・プロファイルがアクセス権限を持つ対象にするドメインを選択します。
   c. 「追加 **(>)**」アイコンをクリックして、ドメインを「割り当て済みのドメイン」ペインに追加します。
   d. 追加するドメインごとに繰り返します。
11. 「保存」をクリックします。

    注**:** セキュリティー・プロファイルに割り当てられているログ・ソースとドメインは、一致する必要があります。ログ・ソースとドメインが一致しない場合は、セキュリティー・プロファイルを保存することはできません。
12. 「セキュリティー・プロファイル管理」ウィンドウを閉じます。
13. 「管理」タブ・メニューで、「変更のデプロイ」をクリックします。

セキュリティー・プロファイルの編集

既存のセキュリティー・プロファイルを編集して、ユーザーがアクセスできるネットワークおよびログ・ソースと、権限の優先順位を更新することができます。

このタスクについて

編集するセキュリティー・プロファイルを「セキュリティー・プロファイル管理」ウィンドウで素早く見つけるには、「入力してフィルタリング」テキスト・ボックスにセキュリティー・プロファイル名を入力します。テキスト・ボックスは、左ペインの上にあります。

手順

1. 「管理」タブをクリックします。

2. ナビゲーション・メニューで、「システム構成」 > 「ユーザー管理」をクリックします。
3. 「セキュリティー・プロファイル **(Security Profiles)**」アイコンをクリックします。
4. 左ペインで、編集するセキュリティー・プロファイルを選択します。
5. ツールバーで、「編集」をクリックします。
6. 必要に応じてパラメーターを更新します。
7. 「保存」をクリックします。
8. 「セキュリティー・プロファイルに時系列データがあります (Security Profile Has Time Series Data)」ウィンドウが表示された場合は、以下のいずれかのオプションを選択します。

オプション	説明
古いデータを保持して保存 **(Keep Old Data and Save)**	以前に集計した時系列データを保存するには、このオプションを選択します。このオプションを選択した場合、このセキュリティー・プロファイルに関連付けられたユーザーが時系列グラフを表示すると、問題が発生する可能性があります。
古いデータを非表示にして保存 **(Hide Old Data and Save)**	時系列データを非表示にするには、このオプションを選択します。このオプションを選択した場合、構成変更のデプロイ後に、時系列データの集計が再開されます。

9. 「セキュリティー・プロファイル管理」ウィンドウを閉じます。
10. 「管理」タブ・メニューで、「変更のデプロイ」をクリックします。

セキュリティー・プロファイルの複製

既存のセキュリティー・プロファイルとほとんど同じ内容の新しいセキュリティー・プロファイルを作成する場合は、既存のセキュリティー・プロファイルをコピーしてから、パラメーターを変更すると便利です。

このタスクについて

コピーするセキュリティー・プロファイルを「セキュリティー・プロファイル管理」ウィンドウで素早く探すには、左ペインの上にある「入力してフィルタリング **(Type to filter)**」テキスト・ボックスにセキュリティー・プロファイル名を入力します。

手順

1. 「管理」タブをクリックします。
2. ナビゲーション・メニューで、「システム構成」 「ユーザー管理」をクリックします。
3. 「セキュリティー・プロファイル **(Security Profiles)**」アイコンをクリックします。
4. 左ペインで、コピーするセキュリティー・プロファイルを選択します。
5. ツールバーで、「コピー」をクリックします。

6. 「確認ウィンドウ」で、複製するセキュリティー・プロファイルの固有名を入力します。
7. 「**OK**」をクリックします。
8. 必要に応じてパラメーターを更新します。
9. 「セキュリティー・プロファイル管理」ウィンドウを閉じます。
10. 「管理」タブ・メニューで、「変更のデプロイ」をクリックします。

セキュリティー・プロファイルの削除

セキュリティー・プロファイルが不要になった場合は、そのセキュリティー・プロファイルを削除してかまいません。

このタスクについて

削除したいセキュリティー・プロファイルにユーザー・アカウントが割り当てられている場合は、そのユーザー・アカウントを別のセキュリティー・プロファイルに再割り当てする必要があります。IBM Security QRadar SIEM は、この状況を自動的に検出して、ユーザー・アカウントを更新するためのプロンプトを表示します。

削除するセキュリティー・プロファイルを「セキュリティー・プロファイル管理」ウィンドウで素早く探すには、「入力してフィルタリング **(Type to filter)**」テキスト・ボックスにセキュリティー・プロファイル名を入力します。テキスト・ボックスは、左ペインの上にあります。

手順

1. 「管理」タブをクリックします。
2. ナビゲーション・メニューで、「システム構成」 > 「ユーザー管理」をクリックします。
3. 「セキュリティー・プロファイル **(Security Profiles)**」アイコンをクリックします。
4. 左ペインで、削除するセキュリティー・プロファイルを選択します。
5. ツールバーで、「削除」をクリックします。
6. 「**OK**」をクリックします。
   - このセキュリティー・プロファイルにユーザー・アカウントが割り当てられている場合は、「ユーザーがこのセキュリティー・プロファイルに割り当てられています (Users are Assigned to this Security Profile)」ウィンドウが開きます。その場合は、 16 ページの『ユーザー・ロールの削除』に進みます。
   - このセキュリティー・プロファイルにユーザー・アカウントが割り当てられていない場合は、セキュリティー・プロファイルが正常に削除されます。その場合は、 16 ページの『ユーザー・ロールの削除』に進みます。
7. リストされているユーザー・アカウントを別のセキュリティー・プロファイルに再割り当てします。
   a. 「割り当てるユーザー・セキュリティー・プロファイル **(User Security Profile to assign)**」リスト・ボックスから、セキュリティー・プロファイルを選択します。
   b. 「確認 **(Confirm)**」をクリックします。

8. 「セキュリティー・プロファイル管理」ウィンドウを閉じます。
9. 「管理」タブ・メニューで、「変更のデプロイ」をクリックします。

ユーザー・アカウント

ユーザー・アカウントは、IBM Security QRadar へのログインに使用される固有のユーザー名を定義し、ユーザーの割り当て先のユーザー・ロール、セキュリティー・プロファイル、およびテナントの割り当てを指定します。

ご使用のシステムを初めて構成する場合は、QRadar にアクセスする必要があるユーザーごとにユーザー・アカウントを作成してください。

ユーザー・アカウントの作成

新しいユーザー・アカウントを作成することができます。

始める前に

ユーザー・アカウントを作成する前に、必要なユーザー・ロールとセキュリティー・プロファイルが作成されていることを確認する必要があります。

このタスクについて

新しいユーザー・アカウントを作成する際に、アクセス資格情報、ユーザー・ロール、セキュリティー・プロファイルをユーザーに割り当てる必要があります。ユーザー・ロールにより、ユーザーが実行権限を持つアクションが定義されます。セキュリティー・プロファイルにより、ユーザーがアクセス権限を持つデータが定義されます。

管理特権を持つ複数のユーザー・アカウントを作成できますが、管理マネージャー・ユーザー・アカウントは、他の管理ユーザー・アカウントを作成することができます。

手順

1. 「管理」タブをクリックします。
2. ナビゲーション・メニューで、「システム構成」 > 「ユーザー管理」をクリックします。
3. 「ユーザー」アイコンをクリックします。
4. 「ユーザー管理」ツールバーで、「新規」をクリックします。
5. 以下のパラメーターの値を入力します。
   a. 「ユーザー名」フィールドに、新規ユーザーの固有のユーザー名を入力します。ユーザー名は 30 文字以内で入力する必要があります。
   b. 「パスワード」フィールドに、アクセスするユーザーのパスワードを入力します。パスワードは、強制される最小の長さと複雑性の要件を満たす必要があります。
6. 「保存」をクリックします。
7. 「ユーザー詳細 (User Details)」ウィンドウを閉じます。
8. 「ユーザー管理」ウィンドウを閉じます。

9. 「管理」タブ・メニューで、「変更のデプロイ」をクリックします。

ユーザー・アカウントの無効化

QRadar へのユーザーのアクセスを制限するためにユーザー・アカウントを無効にすることができます。ユーザー・アカウントを無効にするオプションは、アカウントを削除することなくユーザーのアクセス権限を一時的に取り消します。

このタスクについて

アカウントが無効になっているユーザーがログインしようとすると、ユーザー名とパスワードが無効であることを通知するメッセージが表示されます。ユーザーが作成した項目 (保存済み検索やレポートなど) は、ユーザーに関連付けられたままになります。

手順

1. 「管理」タブをクリックします。
2. ナビゲーション・メニューで、「システム構成」 > 「ユーザー管理」をクリックします。
3. 「ユーザー」アイコンをクリックします。
4. 「ユーザーの管理 (Manage Users)」ペインで、無効にするユーザー・アカウントをクリックします。
5. 「ユーザー詳細 (User Details)」ウィンドウで、「ユーザー・ロール」リストから「無効」を選択します。
6. 「保存」をクリックします。
7. 「ユーザー詳細 (User Details)」ウィンドウを閉じます。
8. 「ユーザー管理」ウィンドウを閉じます。
9. 「管理」タブ・メニューで、「変更のデプロイ」をクリックします。

現在のユーザーに関する情報の表示

製品のメインインターフェースから、現在のユーザーのアカウント情報を表示できます。

手順

1. 右上隅で、ユーザー・アカウント名の横の矢印をクリックします。
2. 「ユーザー設定」をクリックします。
3. オプション: 構成可能なユーザーの詳細を更新します。

オプション	説明
パラメーター	説明
E メール	新しい E メール・アドレスを入力します。
パスワード	新規パスワードを入力します。パスワードは、強制される最小の長さと複雑性の要件を満たす必要があります。
パスワード **(**確認**)**	新規パスワードを再度入力します。

オプション	説明
ポップアップ通知の有効化	ポップアップ・システム通知メッセージは、ユーザー・インターフェースの右下隅に表示されます。ポップアップ通知を無効にするには、このチェック・ボックスをクリアします。

4. 「保存」をクリックします。

ユーザー・アカウントの削除

ユーザー・アカウントが不要になった場合は、そのユーザー・アカウントを削除してかまいません。

このタスクについて

ユーザーを削除すると、そのユーザーはユーザー・インターフェースにアクセスできなくなります。このユーザーがアクセスしようとすると、ユーザー名とパスワードが無効であることを通知するメッセージが表示されます。削除されたユーザーが作成した項目 (保存済み検索やレポートなど) は、削除されたユーザーに関連付けられたままになります。

削除するユーザー・アカウントを「ユーザー管理」ウィンドウで素早く見つけるには、ツールバーの「ユーザーの検索 **(Search User)**」テキスト・ボックスにユーザー名を入力します。

手順

1. 「管理」タブをクリックします。
2. ナビゲーション・メニューで、「システム構成」 > 「ユーザー管理」をクリックします。
3. 「ユーザー」アイコンをクリックします。
4. 削除するユーザーを選択します。
5. ツールバーで、「削除」をクリックします。
6. 「**OK**」をクリックします。
7. 「ユーザー管理」ウィンドウを閉じます。

ユーザー認証

認証が構成され、ユーザーが無効なユーザー名とパスワードの組み合わせを入力すると、ログインが無効であることを示すメッセージが表示されます。

ユーザーが無効な情報を使用して何回かシステムにアクセスしようとする場合、そのユーザーがシステムへのアクセスを再試行するには、構成されている時間だけ待機する必要があります。コンソール設定を構成して、失敗ログインの最大回数とその他の関連する設定を指定することができます。

IBM Security QRadar は、以下の認証タイプをサポートしています。

- システム認証 **(System authentication)** - ユーザーはローカルに認証されます。システム認証はデフォルトの認証タイプです。
- **RADIUS** 認証 **(RADIUS authentication)** - ユーザーは、Remote Authentication Dial-in User Service (RADIUS) サーバーによって認証されます。ユーザーがログインしようとすると、QRadar はパスワードだけを暗号化し、ユーザー名とパスワードを認証用に RADIUS サーバーに転送します。
- **TACACS** 認証 **(TACACS authentication)** - ユーザーは、Terminal Access Controller Access Control System (TACACS) サーバーによって認証されます。ユーザーがログインしようとすると、QRadar はユーザー名とパスワードを暗号化し、この情報を認証用に TACACS サーバーに転送します。TACACS 認証は、TACACS サーバーとして Cisco Secure ACS Express を使用します。QRadar は、Cisco Secure ACS Express 4.3 までをサポートしています。
- **Microsoft Active Directory** - ユーザーは、Kerberos を使用する Lightweight Directory Access Protocol (LDAP) サーバーによって認証されます。
- **LDAP** - ユーザーは、ネイティブの LDAP サーバーによって認証されます。

外部認証プロバイダーの前提条件チェックリスト

RADIUS、TACACS、Active Directory、または LDAP を認証タイプとして構成する前に、以下のタスクを完了する必要があります。

__ • QRadar で認証を構成する前に、認証サーバーを構成します。詳しくは、使用しているサーバーの資料を参照してください。

__ • QRadar と通信するための適切なユーザー・アカウントと特権レベルがサーバー上に存在することを確認します。詳しくは、使用しているサーバーの資料を参照してください。

__ • 認証サーバーの時間と QRadar サーバーの時間が同期していることを確認します。設定時間について詳しくは、 64 ページの『QRadar のシステム時刻』を参照してください。

__ • ベンダー・サーバーでの認証を許可するために、すべてのユーザーが適切なユーザー・アカウントとロールを持っていることを確認します。

QRadar ユーザー・パスワードの変更

IBM Security QRadar は、現在のセキュリティー標準に合わせるために、パスワード・ポリシーを変更する場合があります。パスワード・ポリシーが更新されると、ローカル・パスワードを持つユーザーには、アップグレード後に初めてログインしたときにパスワードの更新を求めるプロンプトが出されます。ごくまれに一部のユーザーにアップグレード後のパスワード変更を求めるプロンプトが出されない場合があるため、管理者はそれらのユーザーのパスワードを変更する必要があります。

SIEM ユーザー・パスワードを変更するには、以下の手順を実行します。

1. 「管理」タブで、「ユーザー管理」セクションの「ユーザー」をクリックします。
2. リストからユーザーを選択し、「編集」をクリックします。
3. 「ユーザーの詳細」ペインで、ユーザーの新規パスワードを入力し、「保存」をクリックします。

4. 変更内容を有効にするには、「管理」タブで「変更のデプロイ」をクリックします。

PCAP ユーザー・パスワードを変更するには、以下の手順を実行します。

1. 「管理」タブで、「システムおよびライセンス管理」をクリックします。
2. 「表示」ドロップダウンから「システム・ビュー **(Systems View)**」を選択します。
3. QRadar Incident Forensics デバイスを強調表示します。
4. 「デプロイメント・アクション」メニューから「ホストの編集」を選択します。
5. 「コンポーネント管理」歯車アイコンを選択します。
6. 「PCAP デバイス管理」ウィンドウで、ユーザーのログイン・パスワードを再入力または変更し、「保存」をクリックします。
7. 「管理」タブで、「拡張」メニューから「すべての構成のデプロイ」を選択して、変更内容を有効にします。

FTP ユーザー・パスワードを変更するには、以下の手順を実行します。

1. 「管理」タブで、「Forensics」セクションの「**Forensics** ユーザー権限」をクリックします。
2. ウィンドウの左側にある「ユーザー」リストからユーザーを選択します。
3. 「ユーザーの編集 **(Edit User)**」ペインで、「**FTP** アクセスを有効にする **(Enable FTP access)**」ボックスにチェック・マークを付けます。
4. ユーザーのパスワードを再入力するか、変更します。
5. 「割り当て済みケース **(Assigned Cases)**」の下の「ユーザーの保存 **(Save User)**」をクリックします。

管理ユーザーの外部認証ガイドライン

外部認証が失敗した場合、管理ユーザーが IBM Security QRadar にログインできなければなりません。

QRadar 管理者ロールでは、外部認証が失敗した場合に備えて、外部認証方式とローカル認証方式の両方が使用可能です。リモート認証が失敗した場合、管理ユーザーはローカル・パスワードを使用してログインできます。外部認証を構成する際に管理ユーザーのローカル・パスワードを設定する必要があります。

ローカル・パスワードはリモート認証局と同期されないため、非管理ユーザーを作成する際にローカル・パスワードは設定されません。非管理ユーザーにとって可能なのは、リモート認証局に対してユーザー名とパスワードを認証することのみです。リモート認証局が無効である場合、または、その他のユーザー資格情報が拒否された場合は、ユーザーはログインできません。

管理ユーザーが QRadar にログインする際にリモート認証ソースが無効であった場合の問題を避けるために、管理ユーザーは、ローカル認証パスワードとリモート認証パスワードの両方を同時に更新する必要があります。リモート認証局がアクティブになっているときにローカル管理パスワードを変更することはできません。管理パスワードを変更するには、以下の手順を実行する必要があります。

1. 外部認証を一時的に無効にします。

2. パスワードをリセットします。
3. 外部パスワードを再構成します。

システム認証の構成

IBM Security QRadar システムでローカル認証を構成することができます。 QRadar V7.3.0.2 以降では、ローカル・パスワードの最小の長さと複雑性の要件を指定できます。

このタスクについて

ローカル認証パスワード・ポリシーは常に、管理ユーザーのローカル・パスワードに適用されます。外部認証が構成されていない場合、このポリシーは非管理ユーザーにも適用されます。

手順

1. 「管理」タブをクリックします。
2. ナビゲーション・メニューで、「システム構成」 > 「ユーザー管理」をクリックします。
3. 「認証」アイコンをクリックします。
4. 「パスワードの最小長」リスト・ボックスで、パスワードで使用しなければならない最小文字数を選択します。

   重要**:** 十分なセキュリティーを提供するには、パスワードに少なくとも 8 文字を含める必要があります。
5. 「パスワードの複雑性の強制」リスト・ボックスで、「はい」または「いいえ」を選択します。 「はい」を選択した場合、パスワードに、大文字、小文字、特殊文字、数字の各属性のうち少なくとも 3 つの属性が含まれている必要があります。特殊文字として、スペース、または英字と数字以外の文字 (例えば、`!"#$%&'()*+,-./:;<=>?@[¥]^_`{|}~`) を使用できます。
6. 「認証モジュール」リスト・ボックスから、「システム認証」を選択します。
7. 「保存」をクリックします。

RADIUS 認証の構成

IBM Security QRadar システムで RADIUS 認証を構成することができます。

手順

1. 「管理」タブをクリックします。
2. ナビゲーション・メニューで、「システム構成」 > 「ユーザー管理」をクリックします。
3. 「認証」アイコンをクリックします。
4. 「認証モジュール」リスト・ボックスから、「**RADIUS** 認証」を選択します。
5. 以下のパラメーターを構成します。
   a. 「**RADIUS** サーバー」フィールドで、RADIUS サーバーのホスト名または IP アドレスを入力します。
   b. 「**RADIUS** ポート」フィールドに、RADIUS サーバーのポートを入力します。

c. 「認証タイプ」リスト・ボックスから、実行する認証のタイプを選択します。

次のオプションから選択してください。

オプション	説明
CHAP	チャレンジ・ハンドシェーク認証プロトコル (CHAP) は、ユーザーとサーバーの間に Point-to-Point Protocol (PPP) 接続を確立します。
MSCHAP	Microsoft チャレンジ・ハンドシェーク認証プロトコル (MSCHAP) は、リモートの Windows ワークステーションを認証します。
ARAP	Apple Remote Access Protocol (ARAP) は、AppleTalk ネットワーク・トラフィックの認証を確立します。
PAP	パスワード認証プロトコル (PAP) は、ユーザーとサーバーの間で平文を送信します。

d. 「共有秘密鍵 **(Shared Secret)**」フィールドに、IBM Security QRadar SIEM が RADIUS サーバーへの伝送用に RADIUS パスワードを暗号化するために使用する共有秘密鍵を入力します。

6. 「保存」をクリックします。

TACACS 認証の構成

IBM Security QRadar システムで TACACS 認証を構成することができます。

手順

1. 「管理」タブをクリックします。
2. ナビゲーション・メニューで、「システム構成」 > 「ユーザー管理」をクリックします。
3. 「認証」アイコンをクリックします。
4. 「認証モジュール」リスト・ボックスから、「**TACACS** 認証」を選択します。
5. 以下のパラメーターを構成します。
   a. 「**TACACS** サーバー」フィールドで、TACACS サーバーのホスト名または IP アドレスを入力します。
   b. 「**TACACS** ポート」フィールドに、TACACS サーバーのポートを入力します。
   c. 「認証タイプ」リスト・ボックスから、実行する認証のタイプを選択します。

次のオプションから選択してください。

オプション	説明
ASCII	情報交換用米国標準コード (ASCII) は、ユーザー名とパスワードを平文で送信します。

オプション	説明
PAP	パスワード認証プロトコル (PAP) は、ユーザーとサーバーの間で平文を送信します。PAP はデフォルトの認証タイプです。
CHAP	チャレンジ・ハンドシェーク認証プロトコル (CHAP) は、ユーザーとサーバーの間に Point-to-Point Protocol (PPP) 接続を確立します。
MSCHAP	Microsoft チャレンジ・ハンドシェーク認証プロトコル (MSCHAP) は、リモートの Windows ワークステーションを認証します。
MSCHAP2	Microsoft チャレンジ・ハンドシェーク認証プロトコル・バージョン 2 (MSCHAP2) は、相互認証を使用してリモートの Windows ワークステーションを認証します。
EAPMD5	MD5 プロトコルを使用する拡張認証プロトコル (EAPMD5) は、MD5 を使用して PPP 接続を確立します。

d. 「共有秘密鍵」フィールドに、QRadar が TACACS サーバーへの伝送用に TACACS パスワードを暗号化するために使用する共有秘密鍵を入力します。

6. 「保存」をクリックします。

Active Directory 認証の構成

IBM Security QRadar システムで Microsoft Active Directory 認証を構成することができます。

手順

1. 「管理」タブをクリックします。
2. ナビゲーション・メニューで、「システム構成」をクリックしてから、「認証」アイコンをクリックします。
3. 「認証モジュール」リスト・ボックスから、「**Active Directory**」を選択します。

以下のパラメーターを構成します。

パラメーター	説明
サーバー URL	LDAP サーバーへの接続に使用される URL を入力します (例: ldaps://*host*:*port*)。
LDAP コンテキスト	使用する LDAP コンテキストを入力します。例えば、DC=QRADAR,DC=INC などです。
LDAP ドメイン	使用するドメインを入力します。例えば、`qradar.inc` などです。

4. 「保存」をクリックします。

LDAP 認証

ユーザー認証/許可にサポート対象の Lightweight Directory Access Protocol (LDAP) プロバイダーを使用するように、IBM Security QRadar を構成することができます。

QRadar は、定義済みの許可基準に基づいて LDAP サーバーからユーザーおよびロール情報を読み取ります。

地理的に分散した環境では、LDAP サーバーと QRadar コンソールがお互い距離的に近い場所にない場合、パフォーマンスに悪影響が生じる可能性があります。例えば、QRadar コンソールが北アメリカにあり、LDAP サーバーがヨーロッパにある場合、ユーザー属性の取り込みに長時間かかることがあります。

LDAP プラグインを使用して、Active Directory サーバーに対して認証を行うことができます。QRadar V7.2.4 以前では、匿名バインドによる認証を許可するようにサーバーを構成する必要があります。ただし、QRadar V7.2.5 以降のバージョンでは、LDAP プラグインにより、Active Directory サーバーに対する認証済みバインドがサポートされています。

QRadar V7.2.4 以降のバージョンでは、ローカル LDAP 認証パスワードを使用します。この方式では、管理者のパスワードがローカルに保管されます。このパスワードは、外部オーセンティケーターが使用できない場合、またはネットワークの問題が原因で LDAP サーバーへの接続が利用できない場合に使用されます。

QRadar V7.2.4 以前では、複数の LDAP サーバー構成はサポートされていません。ただし、QRadar V7.2.5 以降のバージョンでは、複数の LDAP サーバー接続が全面的にサポートされており、新規認証オプションが組み込まれています。

LDAP 認証の構成

IBM Security QRadar システムで LDAP 認証を構成することができます。

始める前に

LDAP サーバーで SSL 暗号化または TLS 認証を使用する場合は、SSL 証明書または TLS 証明書を LDAP サーバーから QRadar コンソールの `/opt/qradar/conf/trusted_certificates` ディレクトリーにインポートする必要があります。証明書の構成について詳しくは、 36 ページの『SSL 証明書または TLS 証明書の構成』を参照してください。

グループ許可を使用する場合は、QRadar ユーザー・ロールまたはセキュリティー・プロファイルを、QRadar が使用する LDAP グループごとに QRadar コンソール上で構成する必要があります。どの QRadar ユーザー・ロールまたはセキュリティー・プロファイルにも、少なくとも 1 つの受け入れグループが必要です。グループ名とユーザー・ロール/セキュリティー・プロファイルのマッピングには、大/小文字の区別があります。

このタスクについて

認証 は、QRadar サーバーにログインしようとするユーザーの身元証明を確立するものです。ユーザーのログイン時には、ユーザー名とパスワードが LDAP ディレクトリーに送信され、資格情報が正しいかどうかが検証されます。この情報を安全に送信するには、Secure Socket Layer (SSL) またはトランスポート層セキュリティー (TLS) の暗号化を使用するように LDAP サーバー接続を構成します。

許可 は、ユーザーが持つアクセス権を確認するプロセスです。ユーザーは各自のロール割り当てに基づいて、タスクの実行を許可されます。許可設定を選択するには、LDAP サーバーへの有効なバインド接続が必要です。

ユーザー属性値には、大/小文字の区別があります。また、グループ名とユーザー・ロール/セキュリティー・プロファイルのマッピングも大/小文字の区別があります。

手順

1. 「管理」タブをクリックします。
2. ナビゲーション・メニューで、「システム構成」 > 「ユーザー管理」をクリックし、「認証」アイコンをクリックします。
3. 「認証モジュール」リスト・ボックスから、「**LDAP**」を選択します。
4. 「追加」をクリックし、基本構成パラメーターを入力します。

LDAP 基本構成パラメーターに関する詳細の説明**:**

表 *5. LDAP* 基本構成パラメーター

パラメーター	説明
サーバー URL	LDAP サーバーの DNS 名または IP アドレス。 URL にはポート値を含める必要があります。 例えば、`ldap://<host_name>:<port>` または `ldap://<ip_address>:<port>` です。
SSL 接続	「**True**」または「**False**」を選択して、Secure Sockets Layer (SSL) 暗号化が有効かどうかを指定します。 SSL 暗号化が有効になっている場合は、「サーバー **URL**」フィールドの値でセキュア接続を指定する必要があります。例えば、`ldaps://secureldap.mydomain.com:636` と指定すると、セキュア・サーバー URL が使用されます。
TLS 認証	「**True**」または「**False**」を選択して、トランスポート層セキュリティー (TLS) 認証が有効かどうかを指定します。 LDAP サーバーに接続するためのトランスポート層セキュリティー (TLS) 暗号化は、通常の LDAP プロトコルの一部としてネゴシエーションされるため、「サーバー **URL**」フィールドに特別なプロトコルやポートを指定する必要はありません。
全体ベースの検索	「**True**」を選択すると、指定したディレクトリー名 (DN) のすべてのサブディレクトリーを検索します。 「**False**」を選択すると、基本 DN 直下の内容を検索します。サブディレクトリーは検索されません。

表 *5. LDAP* 基本構成パラメーター *(*続き*)*

パラメーター	説明
LDAP ユーザー・フィールド	検索対象のユーザー・フィールド ID。 コンマ区切りリストで複数のユーザー・フィールドを指定すると、複数のフィールドを対象にユーザー認証を行うことができます。例えば、**uid,mailid** と指定すると、ユーザー ID とメール ID のどちらを使用してもユーザー認証を行うことができるようになります。
ユーザー基本 DN	ユーザー検索の開始場所となるノードの識別名 (DN)。「ユーザー基本 **DN**」は、ユーザーをロードする際の開始場所となります。パフォーマンス上の理由から、ユーザー基本 **DN** は可能な限り具体的なものにしてください。 例えば、すべてのユーザー・アカウントがディレクトリー・サーバー上の Users フォルダー内にあり、ドメイン名が `ibm.com` の場合、ユーザー基本 DN 値は `cn=Users,dc=ibm,dc=com` となります。
参照	「無視」または「フォロー」を選択して、参照をどのように処理するかを指定します。

5. 「接続設定」で、バインド接続のタイプを選択します。

   バインド接続に関する詳細の説明**:**

表 *6. LDAP* バインド接続

バインド接続タイプ	説明
匿名バインド	認証情報の入力が不要な LDAP ディレクトリー・サーバーとのセッションを作成するには、匿名バインドを使用します。
認証済みバインド	セッションで有効なユーザー名とパスワードの組み合わせを必須とするには、認証済みバインドを使用します。認証済みバインドが成功すると、認証ユーザーに対し、そのセッション中に LDAP ディレクトリーからユーザーおよびロールのリストを読み取る許可が与えられます。セキュリティーを強化するため、バインド接続に使用するユーザー ID には、LDAP ディレクトリーの読み取り以外の操作を行う許可を付与しないようにしてください。 「ログイン **DN**」と「パスワード」を指定します。例えば、ログイン名が `admin`、ドメインが `ibm.com` の場合、「ログイン **DN**」は `cn=admin,dc=ibm,dc=com` となります。

6. 「接続のテスト」をクリックし、接続情報をテストします。 「**LDAP** ユーザー・フィールド」に指定したユーザー属性を対象に認証を行うためのユーザー情報を入力する必要があります。「**LDAP** ユーザー・フィールド」に複数の値を指定している場合は、指定した最初の属性を対象に認証を行うためのユーザー情報を入力する必要があります。
7. 使用する許可方式を選択します。

   許可方式に関する詳細の説明**:**

表 7. *LDAP* 許可方式

許可方式のパラメーター	説明
ローカル	ログインするユーザーごとにユーザー名とパスワードの組み合わせが検証されますが、LDAP サーバーと QRadar サーバーの間で許可情報の交換は行われません。「ローカル」許可を選択している場合は、QRadar コンソールで各ユーザーを作成する必要があります。
ユーザー属性	許可レベルの判別に使用できるユーザー・ロール属性とセキュリティー・プロファイル属性を指定する場合は、「ユーザー属性」を選択します。 ユーザー・ロール属性とセキュリティー・プロファイル属性の両方を指定する必要があります。使用できる属性は、接続設定に基づいて LDAP サーバーから取得されます。ユーザー属性値には、大/小文字の区別があります。
グループ・ベース	LDAP サーバーで認証されたユーザーにロール・ベースのアクセス権を継承させる場合は、「グループ・ベース」を選択します。グループ名とユーザー・ロール/セキュリティー・プロファイルのマッピングには、大/小文字の区別があります。
グループ・ベース DN	グループをロードする際の、LDAP ディレクトリー内の開始ノードを指定します。 例えば、すべてのグループがディレクトリー・サーバー上の `Groups` フォルダー内にあり、ドメイン名が `ibm.com` の場合、「グループ・ベース **DN**」 値は `cn=Groups,dc=ibm,dc=com` となります。
照会制限が有効	返されるグループの数に制限を設定します。
照会結果の限度	照会で返されるグループの最大数。デフォルトでは、最初の 1000 件の照会結果のみが表示されるように制限されています。
メンバーによる	グループ・メンバーに基づいてグループを検索するには、「メンバーによる」を選択します。「グループ・メンバー・フィールド」ボックスで、ユーザー・グループ・メンバーシップの定義に使用する LDAP 属性を指定します。 例えば、グループでグループ・メンバーシップの判別に memberUid 属性が使用される場合、「グループ・メンバー・フィールド」ボックスに `memberUid` と入力します。
照会による	照会を実行してグループを検索するには、「照会による」を選択します。照会情報は、「グループ・メンバー・フィールド」テキスト・ボックスと「グループ照会フィールド」テキスト・ボックスに入力します。 例えば、少なくとも 1 つの **memberUid** 属性を持ち、なおかつ先頭文字が「s」の **cn** 値を持つグループをすべて検索するには、「グループ・メンバー・フィールド」に `memberUid` と入力し、「グループ照会フィールド」に `cn=s*` と入力します。

8. 「グループ・ベース」の許可を指定している場合は、「グループのロード」をクリックし、プラス記号 (+) またはマイナス記号 (-) のアイコンをクリックして、特権グループを追加または削除します。

   ユーザー・ロール特権オプションは、そのユーザーがアクセスできる QRadar コンポーネントを制御します。セキュリティー・プロファイル特権オプションは、各ユーザーがアクセスできる QRadar データを制御します。

   注**:** 「照会制限が有効」チェック・ボックスを選択することにより照会制限を設定することも、LDAP サーバーで照会制限を設定することもできます。LDAP サーバーで照会制限が設定されている場合、「照会制限が有効」チェック・ボックスを選択していなくても、照会制限が有効であることを示すメッセージを受け取ることがあります。
9. 「保存」をクリックします。
10. 「同期の管理」をクリックし、LDAP サーバーと QRadar コンソールの間で認証および許可情報を交換します。
    a. LDAP 接続の構成を初めて行う場合は、「今すぐ同期を実行」をクリックしてデータを同期します。
    b. 自動同期の頻度を指定します。
    c. 「閉じる」をクリックします。
11. 上記のステップを繰り返してさらに LDAP サーバーを追加し、完了したら「保存」をクリックします。

LDAP サーバーとのデータの同期

IBM Security QRadar サーバーと LDAP 認証サーバーの間で、データを手動で同期することができます。

このタスクについて

ユーザー属性またはグループに基づく許可を使用する場合は、ユーザー情報が自動的に LDAP サーバーから QRadar コンソールにインポートされます。

LDAP サーバー上で構成されたグループごとに、それと一致するユーザー・ロールまたはセキュリティー・プロファイルが QRadar コンソール上で構成されている必要があります。一致するグループごとに、ユーザーがインポートされ、そのユーザー・ロールまたはセキュリティー・プロファイルに基づく権限が割り当てられます。

デフォルトでは、同期は 24 時間間隔で実行されます。同期のタイミングは、前回の実行時間に基づいて決まります。例えば、11:45 pm に同期を手動で実行し、同期間隔を 8 時間に設定した場合、次回の同期は 7:45 am に行われます。同期の実行時に、ログイン・ユーザーのアクセス権が変更された場合、セッションが無効になります。ユーザーは、次の要求でログイン画面にリダイレクトされます。

手順

1. 「管理」タブをクリックします。
2. ナビゲーション・メニューで、「システム構成」をクリックします。
3. 「認証」をクリックします。

4. 「認証モジュール」リストで「**LDAP**」を選択します。
5. 「同期の管理」 > 「今すぐ同期を実行」をクリックします。

SSL 証明書または TLS 証明書の構成

ユーザー認証で LDAP ディレクトリー・サーバーを使用し、SSL 暗号化または TLS 認証 を有効にする場合は、SSL 証明書または TLS 証明書を構成する必要があります。

手順

1. SSH を使用して、root ユーザーとしてシステムにログインします。
   a. ユーザー名: root
   b. パスワード: <password>
2. 以下のコマンドを入力して、/opt/qradar/conf/trusted_certificates/ ディレクトリーを作成します。

   ```
   mkdir -p /opt/qradar/conf/trusted_certificates
   ```
3. LDAP サーバーからシステムの /opt/qradar/conf/trusted_certificates ディレクトリーに SSL 証明書または TLS 証明書をコピーします。
4. 証明書ファイル名の拡張子が .cert になっていることを確認します (この拡張子は、その証明書が信頼できることを示します)。 QRadar システムは、.cert ファイルのみをロードします。

LDAP 情報のホバー・テキストの表示

LDAP プロパティー構成ファイルを作成して、LDAP ユーザー情報をホバー・テキストとして表示します。この構成ファイルは、イベント、オフェンス、またはアセットに関連付けられた LDAP ユーザー情報を LDAP データベースに照会します。

始める前に

LDAP プロパティーの作成後に、Web サーバーを再始動する必要があります。システムにログインしているアクティブ・ユーザーのいない保守時間帯に、このタスクをスケジューリングすることを検討してください。

このタスクについて

ldap.properties 構成ファイルに追加できるプロパティーを以下の例にリストします。

```
ldap.url=ldap://LDAPserver.example.com:389
ldap.authentication=simple
ldap.userName=user.name
ldap.password=your.encrypted.password
ldap.basedn=O=IBM,C=US
ldap.filterString=(&(objectclass=user)(samaccountname=%USER%))
ldap.attributes.displayName=Name
ldap.attributes.email=Email
ldap.attributes.employeeID=EmployeeID
ldap.attributes.department=Department
```

手順

1. SSH を使用して、root ユーザーとして IBM Security QRadar にログインします。
2. 暗号化された LDAP ユーザー・パスワードを取得するには、以下の **perl** スクリプトを実行します。

   ```
   perl -I /opt/qradar/lib/Q1/ -e "use auCrypto; print
   Q1::auCrypto::encrypt ('<password>');"
   ```

3. テキスト・エディターを使用して、/opt/qradar/conf/ldap.properties 構成ファイルを作成します。
4. ロケーションと認証情報を指定して、リモート LDAP サーバーにアクセスします。
   a. LDAP サーバーの URL とポート番号を指定します。

      ldaps:// または ldap:// を使用して、リモート・サーバーに接続します。例えば、ldap.url=ldaps://LDAPserver.example.com:389 です。

   b. LDAP サーバーにアクセスするときに使用する認証方式を入力します。

      管理者は、単純な認証方式を使用できます。例えば、ldap.authentication=simple。

   c. LDAP サーバーへのアクセス権限を持つユーザー名を入力します。 例えば、ldap.userName=*user.name*。
   d. リモート LDAP サーバーに対して認証するには、暗号化された LDAP ユーザー・パスワードを入力します。 例えば、ldap.password=*password*。
   e. LDAP サーバーでユーザーを検索するために使用する基本 DN を入力します。 例えば、ldap.basedn=*BaseDN*。
   f. LDAP 内で検索パラメーター・フィルターに使用する値を入力します。

      例えば QRadar では、ldap.filterString=(&(objectclass=user)(samaccountname=%USER%)) の上にポインターを置くと、%USER% 値がユーザー名に置き換えられます。

5. ホバー・テキストに表示する属性を 1 つ以上入力します。

   少なくとも 1 つの LDAP 属性を含める必要があります。各値は、ldap.attributes.*AttributeName=UI* に表示する説明テキスト の形式を使用する必要があります。

6. ldap.properties 構成ファイルに対する読み取りレベルのアクセス権があることを確認します。
7. QRadar に管理者としてログインします。
8. 「管理」タブで、「拡張」 > 「**Web** サーバーの再始動」を選択します。

タスクの結果

管理者が「ログ・アクティビティー」タブおよび「オフェンス」タブの「ユーザー名」フィールドまたは「アセット」タブ (使用可能な場合) の「最後のユーザー」フィールドにポインターを置くと、LDAP ユーザーに関する詳細情報を表示できるようになります。

複数の LDAP リポジトリー

複数の LDAP リポジトリーの項目を 1 つの仮想リポジトリーにマップするように IBM Security QRadar を構成できます。

複数のリポジトリーが構成されている場合、ユーザーはログイン時に認証に使用するリポジトリーを指定する必要があります。その場合、ユーザー名フィールドでリポジトリーの絶対パスとドメイン名を指定する必要があります。例えば、Repository_1 がドメイン ibm.com を、Repository_2 が ドメイン ibm.ca.com を使用するように構成されている場合、ログイン情報は以下の例のようになります。

- OU=User Accounts,OU=PHX,DC=qcorpaa,DC=aa,DC=ibm.com¥*username*
- OU=Office,OU=User Accounts,DC=qcorpaa,DC=aa,DC=ibm.ca.com¥*username*

ユーザー属性またはグループ許可を使用するリポジトリーには、LDAP サーバーからユーザー情報が自動インポートされます。ローカル許可を使用するリポジトリーについては、QRadar システム上でユーザーを直接作成する必要があります。

例: 最小特権アクセスの構成と設定

日常的なタスクを実行するのに必要な最小限のアクセス権限のみをユーザーに付与します。

IBM Security QRadar データと QRadar の諸機能に異なる特権を割り当てることができます。この割り当てを行うには、各セキュリティー・プロファイルと各ユーザー・ロールに対して異なる受け入れ/拒否グループを指定します。受け入れグループは特権を割り当て、拒否グループは特権を制限します。

例を見て見ましょう。会社が学生インターンのグループを雇用したとします。John は、地元の大学でサイバー・セキュリティー・プログラムを専攻している最終学年の学生です。彼はネットワークの既知の脆弱性をモニターして確認し、調査結果に基づいて修復計画を作成するよう依頼されました。企業のネットワーク脆弱性に関する情報は機密情報です。

QRadar 管理者は、学生インターンのデータとシステムへのアクセスが制限されていることを確認する必要があります。ほとんどの学生インターンは IBM Security QRadar Vulnerability Manager へのアクセスが拒否されなければなりませんが、John の特殊な職務にはこのアクセス権限が必要です。組織のポリシーでは、学生インターンが QRadar API へのアクセス権限を持つことを許可していません。

次の表は、John は IBM Security QRadar Risk Manager と QRadar Vulnerability Manager にアクセスするには **company.interns** グループと**qvm.interns** グループに所属している必要があることを示します。

表 *8.* ユーザー・ロール特権グループ

ユーザー・ロール	受け入れ	拒否
管理	**qradar.admin**	**company.firedemployees**
QVM	**qradar.qvm** **qvm.interns**	**company.firedemployees** **qradar.qrm** **company.interns**

表 *8.* ユーザー・ロール特権グループ *(*続き*)*

ユーザー・ロール	受け入れ	拒否
QRM	**qradar.qrm** **company.interns**	**company.firedemployees**

次の表は、**qvm.interns** のセキュリティー・プロファイルによって John が QRadar API へのアクセスを制限されていることを示します。

表 *9.* セキュリティー・プロファイル特権グループ

セキュリティー・プロファイル	受け入れ	拒否
QVM	**qradar.secprofile.qvm**	**company.firedemployees**
API	**qradar.secprofile.qvm.api**	**company.firedemployees** **qradar.secprofile.qvm.interns**

第 4 章 ライセンス管理

ライセンス・キーは、特定の IBM Security QRadar 製品に対する資格を付与し、QRadar デプロイメント環境のイベントおよびフローのキャパシティーを制御します。ライセンスをデプロイメント環境に追加して、他の QRadar 製品 (QRadar Vulnerability Manager など) をアクティブにできます。

QRadar をインストールしたときのデフォルトのライセンス・キーは一時的なものです。このキーにより、インストール日から 35 日間、システムへのアクセス権限が付与されます。QRadar のご購入時に IBM から届く E メールに、永久ライセンス・キーが記載されています。このライセンス・キーにより、アプライアンスの機能が拡張されます。デフォルトのライセンスが期限切れになる前に、このライセンス・キーを適用する必要があります。

ライセンス・キーをシステムに適用するには、以下の手順を実行します。

1. ライセンス・キーを取得します。新しいライセンス・キーまたは更新されたライセンス・キーについては、営業担当員にお問い合わせください。
2. ライセンス・キーをアップロードします。
3. システムにライセンスを割り振ります。
4. すべての構成をデプロイします。

ライセンス・キーを QRadar に適用した後、EPS レートおよび FPM レートの再配分を行うことで、ネットワーク・トラフィックの平均量を処理するのに十分なキャパシティーが各管理対象ホストに割り振られる一方で、各管理対象ホストは、データ・スパイクを効率的に処理するのに十分な EPS および FPM を引き続き維持します。EPS および FPM のキャパシティーを再配分した後、変更内容をデプロイする必要はありません。

ライセンスの有効期限

システムの処理能力は、QRadar がリアルタイムに処理できるイベントおよびフローの量によって測定されます。処理能力は、アプライアンス・ハードウェアまたはライセンス・キーによって制限される場合があります。一時ライセンス・キーの場合、QRadar コンソール では 1 秒当たりのイベント数 (EPS) として 5,000、管理対象ホストでは 10,000 EPS が対応可能です。QRadar コンソールおよび管理対象ホストの両方で、一時ライセンスの場合の FPM レートは 200,000 です。

ライセンスの有効期限が切れたとき、QRadar はライセンス交付を受けたキャパシティーの上限までイベントおよびフローの処理を続けます。期限切れライセンスの EPS および FPM のキャパシティーがホストに割り振られていた場合、共有ライセンス・プールが不足し、QRadar が「ネットワーク・アクティビティー」タブおよび「ログ・アクティビティー」タブの機能のブロックを引き起こす可能性があります。

QRadar で処理される着信ネットワークのデータの量に対してライセンスが交付されていない場合は、イベントまたはフローのキャパシティーがより多いライセンスを追加することができます。

関連概念:

5 ページの『IBM Security QRadar 製品の機能』
IBM Security QRadar 製品資料では、オフェンス、フロー、アセット、ヒストリカル相関などの機能について説明していますが、すべての QRadar 製品でこれらの機能を利用できるわけではありません。使用する製品によっては、説明されている一部の機能をデプロイメントで使用できない場合があります。各製品の機能を確認して、必要な情報を入手してください。

55 ページの『第 5 章 システム管理』
IBM Security QRadar は、さまざまなサイズとトポロジーのデプロイメントをサポートするモジュラー・アーキテクチャーになっています。

イベントおよびフローの処理能力

デプロイメント環境のキャパシティーは、IBM Security QRadar がリアルタイムで収集、正規化、および相関付け可能な 1 秒当たりのイベント数 (EPS) と 1 分当たりのフロー数 (FPM) で測定します。イベントおよびフローのキャパシティーは、システムにアップロードされるライセンスによって設定されます。

QRadar が受信データ・スパイクを処理できるようにするには、QRadar デプロイメント内の各ホストに十分なイベントおよびフローのキャパシティーがなければなりません。ほとんどの受信データ・スパイクは一時的なものですが、システムがライセンス・キャパシティーを超過していることを示すシステム通知を繰り返し受け取る場合は、既存のライセンスを、より大きな EPS または FPM のキャパシティーを備えたライセンスに置き換えることができます。

関連概念:

45 ページの『バーストの処理』
IBM Security QRadar はバーストの処理を使用して、割り当てられた、1 秒あたりのイベント数 (EPS) または 1 分あたりのフロー数 (FPM) のライセンス制限をシステムが超過したときにデータが損失しないようにします。

関連タスク:

49 ページの『イベントおよびフローのキャパシティーの配分』
「ライセンス・プール管理」ウィンドウを使用して、使用権限が付与されている EPS (1 秒当たりのイベント数) と FPM (1 分当たりのフロー数) をすべて使用するようにデプロイメントが構成されていることを確認します。また、イベントやフローをドロップしたり、未使用の EPS および FPM が過剰に発生したりすることなくデータの周期的バーストを処理するように、IBM Security QRadar を適切に構成します。

共有ライセンス・プール

各ライセンスによって設定された EPS レートおよび FPM レートは、共有ライセンス・プールに結合されます。元のライセンスがどのホストに割り振られているかに関係なく、共有ライセンス・プールから任意のホストに処理能力を分散できます。

共有ライセンス・プールの割り振りを調整することにより、イベントおよびフローのキャパシティーがネットワーク・ワークロードに応じて分散されて、各 QRadar ホストが、ピーク・トラフィックの期間を効率的に管理するために十分な EPS および FPM を持つようにできます。

個別のイベント・コレクター・アプライアンスとイベント・プロセッサー・アプライアンスが存在するデプロイメント環境では、イベント・コレクターが接続されているイベント・プロセッサーの EPS レートが、そのイベント・コレクターに継承されます。イベント・コレクターの処理能力を上げるには、共有ライセンス・プールから親イベント・プロセッサーに割り振られる EPS を大きくします。

ライセンス・プールへの提供

イベントおよびフローの両方のキャパシティーを含むライセンスは、必ずしも EPS と FPM の両方を共有ライセンス・プールに提供するとは限りません。ライセンス・プールの提供は、そのライセンスが割り振られているアプライアンスのタイプに依存します。例えば、ライセンスを 16xx イベント・プロセッサーに適用すると、EPS のみがライセンス・プールに追加されます。同じライセンスを、17xx フロー・プロセッサーに適用すると、FPM のみがライセンス・プールに提供されます。このライセンスを 18xx イベント/フロー・プロセッサーに適用すると、EPS と FPM の両方がプールに提供されます。

イベント・コレクターまたはフロー・コレクターのソフトウェア・ライセンスを除くすべてのソフトウェア・ライセンスは、ライセンスが割り振られているアプライアンスのタイプに関係なく、EPS と FPM の両方を共有ライセンス・プールに提供します。

シリアル番号があるライセンス・キーは 1 つのホストのみに適用でき、そのライセンスの EPS および FPM のキャパシティーは別のホストに割り振ることはできません。結果として、シリアル番号があるライセンス・キーは共有ライセンス・プールに提供されません。

ライセンス交付を受けた処理能力の制限の超過

管理対象ホストに割り振られている EPS と FPM の組み合わせが、共有ライセンス・プール内の EPS と FPM を超えると、ライセンス・プールが割り振り超過になります。ライセンス・プールが割り振り超過のときは、「ライセンス・プール管理」ウィンドウで EPS および FPM に負の値が表示され、割り振りグラフが赤に変わります。QRadar は、「ネットワーク・アクティビティー」タブおよび「ログ・アクティビティー」タブの機能をブロックします。これには、メインの QRadar ツールバー上の「メッセージ」リストからイベントおよびフローを表示する機能も含まれます。

ブロックされた機能を使用可能にするには、デプロイメント環境内の管理対象ホストに割り振った EPS および FPM を削減します。既存のライセンスに、ネットワーク・データ量を処理するのに十分なイベントおよびフローのキャパシティーがない場合は、共有ライセンス・プール内の不足を解決するのに十分な EPS または FPM を含む新しいライセンスをアップロードします。

期限切れライセンス

ライセンスの有効期限が切れても、QRadar は割り振られたレートでイベントおよびフローの処理を続行します。

期限切れライセンスの EPS および FPM のキャパシティーがホストに割り振られていた場合、ライセンス・プール内の共有リソースが不足し、QRadar が「ネットワーク・アクティビティー」タブおよび「ログ・アクティビティー」タブの機能をブロックする原因になる可能性があります。

キャパシティー・サイズ設定

データのスパイクを処理する最善の方法は、受信データのピーク期間のバランスを取るために十分な 1 秒当たりのイベント数 (EPS) と 1 分当たりのフロー数 (FPM) をデプロイメントに確実に設定することです。その目的は、ホストがデータ・スパイクを効率的に処理するために十分なキャパシティーを持つが、アイドルの EPS および FPM を大量には持たないように、EPS および FPM を割り振ることです。

ライセンス・プールから割り振られた EPS または FPM がアプライアンスの平均 EPS または FPM に非常に近い場合、システムは、後で処理されるようにデータを一時キューに累積する可能性があります。一時キュー (バースト処理キューとも呼ばれます) にデータが多く累積するほど、QRadar がバックログを処理する時間は長くなります。例えば、割り振られたレートが 10,000 EPS である QRadar ホストが、ホストの平均 EPS レートが 9,500 である場合にバースト処理キューを空にするには、平均 EPS レートが 7,000 であるシステムと比べてより長い時間がかかります。

オフェンスは、データがアプライアンスによって処理されるまで生成されないため、QRadar がバースト処理キューにデータを追加する頻度を最少にすることが重要です。各管理対象ホストが短期間のデータ・バーストを処理するために十分なキャパシティーを確実に持つようにすることで、QRadar がキューを処理するためにかかる時間を最小化し、イベントの発生時にオフェンスが作成されるようにします。

割り振られた処理能力をシステムが継続的に超える場合は、キュー・サイズを増やしても問題は解決できません。超過データは、処理されるために待機が必要なバースト処理キューの末尾に追加されます。キューが大きいほど、キューに入れられたイベントがアプライアンスによって処理される時間は長くなります。

関連概念:

45 ページの『例: 受信データ・スパイク』

毎朝 8 時から 9 時の間、従業員がログインしてネットワーク・リソースを使用し始めるため、会社のネットワークでデータ・スパイクが発生します。

内部イベント

IBM Security QRadar アプライアンスは、それらのアプライアンスがデータ処理時に相互に通信する際に少数の内部イベントを生成します。

割り振られたキャパシティーの対象として内部イベントがカウントされないように、システムは、内部イベントが生成された直後にそのすべてのイベントをライセンス・プールに自動的に返します。

バーストの処理

IBM Security QRadar はバーストの処理を使用して、割り当てられた、1 秒あたりのイベント数 (EPS) または 1 分あたりのフロー数 (FPM) のライセンス制限をシステムが超過したときにデータが損失しないようにします。

割り当てられた EPS 制限および FPM 制限を超過する原因となるデータ・スパイクを QRadar が受信すると、超過分のイベントおよびフローは、受信データ・レートが低下した際に処理されるように一時キューに移動されます。バーストの処理がトリガーされると、システム通知により、アプライアンスで EPS または FPM のライセンス制限が超過したことを示すアラートが出されます。

一時キュー内のバックログは、それらのイベントまたはフローの受信順に処理されます。キューの最初にある古いデータは、キューの最後にある最新データより先に処理されます。キューが空または満杯になる速度は、いくつかの要因 (データ・スパイクのボリュームおよび期間、アプライアンスのキャパシティー、ペイロードのサイズなど) の影響を受けます。

バーストのリカバリー・レートは、割り当てられているレートと、受信レートとの間の差です。受信データのボリュームが低下すると、システムは、リカバリー・レートが許容する速さでキュー内のイベントまたはフローのバックログを処理します。リカバリー・レートが低いほど、キューが空になるまでの時間が長くなります。

関連概念:

42 ページの『イベントおよびフローの処理能力』

QRadar が受信データ・スパイクを処理できるようにするには、QRadar デプロイメント内の各ホストに十分なイベントおよびフローのキャパシティーがなければなりません。ほとんどの受信データ・スパイクは一時的なものですが、システムがライセンス・キャパシティーを超過していることを示すシステム通知を繰り返し受け取る場合は、既存のライセンスを、より大きな EPS または FPM のキャパシティーを備えたライセンスに置き換えることができます。

関連タスク:

49 ページの『イベントおよびフローのキャパシティーの配分』

「ライセンス・プール管理」ウィンドウを使用して、使用権限が付与されている EPS (1 秒当たりのイベント数) と FPM (1 分当たりのフロー数) をすべて使用するようにデプロイメントが構成されていることを確認します。また、イベントやフローをドロップしたり、未使用の EPS および FPM が過剰に発生したりすることなくデータの周期的バーストを処理するように、IBM Security QRadar を適切に構成します。

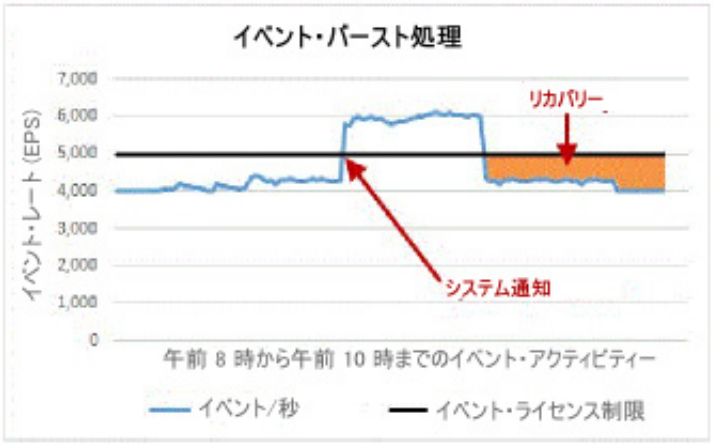
例: 受信データ・スパイク

毎朝 8 時から 9 時の間、従業員がログインしてネットワーク・リソースを使用し始めるため、会社のネットワークでデータ・スパイクが発生します。

この会社のデプロイメント環境には、割り振られた 1 秒当たりのイベント数 (EPS) が 5,000 および 1 分当たりのフロー数 (FPM) が 100,000 の QRadar 1828 Event/Flow Processor アプライアンスが組み込まれています。このアプライアンスの平均キャパシティーは、4,000 EPS と 70,000 FPM です。

データ・スパイク時 (午前 9 時ごろがピーク) に、アプライアンスはいつも最大で 6,000 EPS および 120,000 FPM を受信します。QRadar は、超過分のイベントおよびフロー (1,000 EPS および 20,000 FPM) をバースト処理キューに自動的に移動し、割り振られたキャパシティーをアプライアンスが超えたことを管理者にアラートするためにシステム通知を生成します。

以下の図は、受信イベントおよび受信フローのデータが、ライセンス交付を受けたキャパシティーを超過したときの 2 時間の枠を示しています。超過すると、システム通知がトリガーされます。また、データ量が平常に戻った後のリカバリー期間も示しています。



リカバリー・レートは、割り振られた EPS または FPM の量と、現在の受信データ・レートとの間の差です。この例では、イベント・レートおよびフロー・レートが平常に戻ったとき、リカバリー・レートは 1,000 EPS と 30,000 FPM です。

```
5,000 licensed events - 4,000 incoming events = 1,000 EPS recovery rate
100,000 licensed flows - 70,000 incoming flows = 30,000 FPM recovery rate
```

オフェンスは、データがアプライアンスによって処理されるまで生成されないため、データ・スパイクから素早くリカバリーできるようにするのに十分な EPS と FPM をアプライアンスに割り振ることが重要です。

関連概念:

44 ページの『キャパシティー・サイズ設定』
データのスパイクを処理する最善の方法は、受信データのピーク期間のバランスを取るために十分な 1 秒当たりのイベント数 (EPS) と 1 分当たりのフロー数 (FPM) をデプロイメントに確実に設定することです。その目的は、ホストがデータ・スパイクを効率的に処理するために十分なキャパシティーを持つが、アイドルの EPS および FPM を大量には持たないように、EPS および FPM を割り振ることです。

関連タスク:

49 ページの『イベントおよびフローのキャパシティーの配分』
「ライセンス・プール管理」ウィンドウを使用して、使用権限が付与されている EPS (1 秒当たりのイベント数) と FPM (1 分当たりのフロー数) をすべて使用するようにデプロイメントが構成されていることを確認します。また、イベントやフローをドロップしたり、未使用の EPS および FPM が過剰に発生したりすることなくデータの周期的バーストを処理するように、IBM Security QRadar を適切に構成します。

ライセンス・キーのアップロード

ライセンス・キーは、IBM Security QRadar 製品および機能に対するライセンス資格、さらにはイベントおよびフローを処理するシステム・キャパシティーに対するライセンス資格を決定します。

始める前に

新しいライセンス・キーまたは更新されたライセンス・キーの取得について支援が必要な場合は、営業担当員にお問い合わせください。

このタスクについて

以下のタスクを実行するときには、ライセンス・キーをアップロードする必要があります。

- 有効期限が切れた QRadar コンソール・ライセンスの更新
- 1 秒あたりのイベント数 (EPS) または 1 分あたりのフロー数 (FPM) の制限の引き上げ
- デプロイメントへの IBM Security QRadar Vulnerability Manager などの QRadar 製品の追加

QRadar V7.3.0 では、イベント・プロセッサーまたはフロー・プロセッサーをデプロイメント環境に追加するときに、新しいライセンスをアップロードする必要はありません。イベント・プロセッサーおよびフロー・プロセッサーには無期限のアプライアンス・ライセンスが自動的に割り当てられるため、ライセンス・プールからアプライアンスに EPS または FPM を割り振ることができます。

ログオンしたときに QRadar コンソールのライセンス・キーの有効期限が切れていた場合は、自動的に「システムおよびライセンス管理」ウィンドウが表示されます。操作を続行するには、ライセンス・キーをアップロードする必要があります。

管理対象ホスト・システムでライセンス・キーの有効期限が切れている場合は、ログイン時に、管理対象ホスト・システムで新しいライセンス・キーが必要であることを通知するメッセージが表示されます。「システムおよびライセンス管理」ウィンドウを使用して、ライセンス・キーを更新します。ライセンス・プールが割り振り制限を超えていない場合は、有効期限が切れたキーを削除し、ライセンス・プールから管理対象ホストに EPS または FPM を割り振ります。

手順

1. 「管理」タブで、「システムおよびライセンス管理」アイコンをクリックします。
2. ツールバーで、「ライセンスのアップロード」をクリックします。
3. ダイアログ・ボックスで、「ファイルの選択」をクリックします。
4. ライセンス・キーを選択し、「オープン」をクリックします。
5. 「アップロード」をクリックし、「確認」をクリックします。

タスクの結果

ライセンスが QRadar コンソールにアップロードされ、「システムおよびライセンス管理」ウィンドウに表示されます。

デフォルトでは、ほとんどのライセンスは、QRadar ホストに即時に割り振られません。ただし、QRadar Vulnerability Manager、QRadar Risk Manager、および QRadar Incident Forensics のキーはいずれも、システムによって QRadar コンソールに自動的に割り振られます。

次のタスク

システムにライセンスを割り振ります。

ホストへのライセンス・キーの割り振り

既存のライセンスを置き換える場合、新しい QRadar 製品を追加する場合、または共有ライセンス・プール内のイベントまたはフローのキャパシティーを増やす場合は、ライセンス・キーを IBM Security QRadar ホストに割り振ります。

始める前に

ライセンス・キーをアップロードする必要があります。

このタスクについて

複数のライセンスを 1 つの QRadar コンソールに割り振ることができます。例えば、IBM Security QRadar Risk Manager と QRadar Vulnerability Manager を追加するライセンス・キーを QRadar コンソールに割り振ることができます。

ライセンス・キーを QRadar ホストに追加した後は、そのライセンス・キーを取り消すことはできません。誤ってライセンスを間違ったホストに割り振った場合は、変更内容をデプロイした後に、システムからそのライセンスを削除する必要があります。ライセンスを削除すると、ライセンスを再度アップロードして再割り振りすることができます。ライセンスを正しいホストに割り振った後、変更内容を再度デプロイする必要があります。

手順

1. 「管理」タブで、「システムおよびライセンス管理」アイコンをクリックします。
2. 「表示」リストから、「ライセンス」を選択します。
3. ライセンスを選択して、「ライセンスへのシステムの割り振り」をクリックします。

   ヒント: 「表示」リストで「システム」を選択すると、ラベルが「システムへのライセンスの割り振り」に変わります。
4. ライセンスのリストをフィルタリングするには、検索ボックスにキーワードを入力します。
5. 「ライセンスへのシステムの割り振り」ウィンドウで、ライセンスを割り振るホストを選択し、「ライセンスへのシステムの割り振り」をクリックします。

イベントおよびフローのキャパシティーの配分

「ライセンス・プール管理」ウィンドウを使用して、使用権限が付与されている EPS (1 秒当たりのイベント数) と FPM (1 分当たりのフロー数) をすべて使用するようにデプロイメントが構成されていることを確認します。また、イベントやフローをドロップしたり、未使用の EPS および FPM が過剰に発生したりすることなくデータの周期的バーストを処理するように、IBM Security QRadar を適切に構成します。

始める前に

ライセンス・プールに十分な数の未割り振りの EPS と FPM が存在することを確認します。ライセンス・プール内の EPS または FPM がすべて割り振られている場合は、割り振りを再配分してください。

このタスクについて

QRadar がすべてのイベントおよびフローを適切なタイミングで処理するためには、EPS および FPM のキャパシティーを適切に割り振ることが重要です。目的は、使用されていない EPS および FPM のキャパシティーが必要以上に多くならないようにして、データ・スパイクを効率的に処理できるだけの十分なキャパシティーをホストが持つように EPS および FPM を割り振ることです。

手順

1. 「管理」タブで、「システムおよびライセンス管理」アイコンをクリックします。
2. 「表示」リストから、「ライセンス」を選択します。

3. 「ライセンス・プール管理」をクリックし、円グラフの上にマウス・ポインターを移動して、デプロイメントの合計キャパシティーを表示します。
4. 「ライセンス割り振り」テーブルで、データを検討して、平均的な EPS と FPM に対応するために十分なイベントおよびフローのキャパシティーがアプライアンスにあり、なおかつピーク時のボリュームに対応するために十分なキャパシティーが残っているかどうかを判別します。

   イベントおよびフローのキャパシティー・データの検討に関する詳細の説明**:**

   - 「**EPS** 割り振り」列と「**FPM** 割り振り」列には、各 QRadar プロセッサーまたは QRadar コンソールに割り当てられているキャパシティーが表示されます。
   - 「平均 **EPS**」列と「平均 **FPM**」列には、過去 30 日間に QRadar ホストによって処理されたイベントおよびフローの平均数が表示されます。この計算では、「イベント・レート **(EPS)**」保存済み検索および「フロー・レート **(FPS)**」保存済み検索が使用されます。保存済み検索が削除されているデプロイメント環境では、イベント・レートおよびフロー・レートの平均は「**N/A**」と表示されます。「イベント・レート **(EPS)**」保存済み検索および「フロー・レート **(FPS)**」保存済み検索を再インポートするには、IBM Security App Exchange から **IBM Security Baseline Maintenance Content** Extension V1.0.2 以降をインストールしてください。
   - ホスト名をクリックして、過去 30 日間のピーク EPS とピーク FPM のレートの詳細を表示します。
5. QRadar ホストの割り振り済み EPS レートまたは割り振り済み FPM レートを変更するには、編集アイコンをクリックします。
6. 「割り振り済み **EPS**」フィールドまたは「割り振り済み **FPM**」フィールドを更新し、「保存」をクリックします。 変更された EPS 割り振りおよび FPM 割り振りは、以下の基準に基づいて検証されます。
   - EPS 割り振りは 100 の倍数である必要があり、FPM 割り振りは 5,000 の倍数である必要があります。
   - 割り振られた EPS または FPM によりライセンス・プールが割り振り過剰になることがない。
   - 割り振られた EPS または FPM が、当該アプライアンス・タイプのハードウェア制限を超えていない。

関連概念:

45 ページの『例: 受信データ・スパイク』
毎朝 8 時から 9 時の間、従業員がログインしてネットワーク・リソースを使用し始めるため、会社のネットワークでデータ・スパイクが発生します。

45 ページの『バーストの処理』
IBM Security QRadar はバーストの処理を使用して、割り当てられた、1 秒あたりのイベント数 (EPS) または 1 分あたりのフロー数 (FPM) のライセンス制限をシステムが超過したときにデータが損失しないようにします。

42 ページの『イベントおよびフローの処理能力』
QRadar が受信データ・スパイクを処理できるようにするには、QRadar デプロイメント内の各ホストに十分なイベントおよびフローのキャパシティーがなければなりません。ほとんどの受信データ・スパイクは一時的なものですが、システムがライセンス・キャパシティーを超過していることを示すシステム通知を繰り返し受け取る場合は、既存のライセンスを、より大きな EPS または FPM のキャパシティーを備えたライセンスに置き換えることができます。

ライセンスの詳細の表示

システムにアップロードされている各ライセンスの状況、有効期限、イベント・レート制限、フロー・レート制限などの情報を参照するには、ライセンスの詳細を表示します。

このタスクについて

ホストにまだ割り振られていないライセンスは、「ライセンス」表の上部に表示されます。デプロイメント環境内の各ホストには、太字で表示されるサマリーの行があります。サマリーの行の「イベント・レート制限」フィールドと「フロー・レート制限」フィールドには、ホストに割り振られている EPS および FPM が表示されます。ホストに割り振られている EPS および FPM がない場合、「イベント・レート制限」列と「フロー・レート制限」列には、「**N/A**」が表示されます。

QRadar ホストに割り振られているライセンスは、QRadar ホストのサマリーの行の下にネストされた子の行として表示されます。QRadar コンソール、イベント・プロセッサー、およびフロー・プロセッサーのアプライアンスの場合、子の行には、ライセンスの EPS および FPM の部分のキャパシティーと有効期限が表示されます。ライセンスを管理するためには、個別ライセンスに対応する行を選択します。

手順

1. 「管理」タブで、「システムおよびライセンス管理」アイコンをクリックします。
2. 「表示」リストから、「ライセンス」を選択します。
3. 特定のホストまたはライセンスに関する詳細情報を表示するには、ネストされた行を選択し、「アクション」 > 「ライセンスの表示」をクリックします。

表 *10. QRadar* ライセンスの状況

状態	説明
未割り振り	ライセンスはアップロードされていますが、QRadar ホストに割り振られていません。ライセンスの EPS および FPM はライセンス・プールに提供されません。
未デプロイ	ライセンスは QRadar ホストに割り振られていますが、デプロイされていません。ライセンスは、デプロイメント環境内でまだアクティブになっていません。EPS および FPM はライセンス・プールに含まれます。
デプロイ済み	ライセンスは割り振り済みで、デプロイメント環境内でアクティブになっています。EPS および FPM はライセンス・プールに含まれます。

有効期限が切れたライセンスの削除

間違った QRadar ホストにライセンスを誤って割り振った場合、ライセンスを削除します。また、有効期限が切れたライセンスを削除して、IBM Security QRadar がその期限切れライセンスに関して生成する日次のシステム通知を停止します。

このタスクについて

削除によってライセンス・プールが割り振り制限を超える場合、ライセンスを削除することはできません。QRadar は、ライセンスを削除したときにキャパシティー低下に対応できるだけの十分な未割り振りの EPS および FPM のキャパシティーがライセンス・プールにあるかどうかを検証します。例えば、2,500 EPS が関連付けられているライセンスを削除する場合、ライセンス・プールには、QRadar ホストに割り振られていない EPS が少なくとも 2,500 存在していなければなりません。

不足分に対応できるだけの十分な未割り振りの EPS および FPM がライセンス・プールにない場合は、ライセンスを削除したときにライセンス・プールが割り振り制限を超えないように EPS および FPM の割り振りを調整する必要があります。

手順

1. 「管理」タブで、「システムおよびライセンス管理」アイコンをクリックします。
2. 「表示」リストから、「ライセンス」を選択します。
3. ホストの表で、削除するライセンスを含む、ネストされた子の行を選択します。
4. 「アクション」 > 「ライセンスの削除」をクリックします。

   「ライセンスの有効期限」には「無期限」が表示され、「イベント・レート制限」と「フロー・レート制限」には 0 が表示されます。

ライセンス情報のエクスポート

監査の目的で、システムにインストールされているライセンス・キーに関する情報を外部の .xml ファイルにエクスポートします。

.xml ファイルを使用してライセンスを別のシステムに移動することはできません。このファイルは、個々のライセンス・キーに関する詳細情報を表示する目的でのみ使用してください。

手順

1. 「管理」タブをクリックします。
2. ナビゲーション・メニューで、「システム構成」をクリックします。
3. 「システムおよびライセンス管理」アイコンをクリックします。
4. 「表示」リストから、「ライセンス」を選択します。
5. 「アクション」メニューから、「ライセンスのエクスポート **(Export Licenses)**」を選択します。

6. ファイルをローカルの場所に保存し、「**OK**」をクリックします。

第 5 章 システム管理

IBM Security QRadar は、さまざまなサイズとトポロジーのデプロイメントをサポートするモジュラー・アーキテクチャーになっています。

単一ホストのデプロイメント環境では、すべてのソフトウェア・コンポーネントが単一アプライアンス上で実行され、QRadar コンソール により、ユーザー・インターフェース、リアルタイムのイベントとフローの表示、レポート、オフェンス、アセット情報、および管理機能が提供されます。

QRadar を拡張するために、コンソールでない管理対象ホストをデプロイメントに追加できます。各管理対象ホストに対して特定のコンポーネント・タイプ (コレクター、プロセッサー、データ・ノードなど) を構成でき、分散環境でのデータ収集およびデータ処理の柔軟性が大幅に向上します。

関連概念:

41 ページの『第 4 章 ライセンス管理』
ライセンス・キーは、特定の IBM Security QRadar 製品に対する資格を付与し、QRadar デプロイメント環境のイベントおよびフローのキャパシティーを制御します。ライセンスをデプロイメント環境に追加して、他の QRadar 製品 (QRadar Vulnerability Manager など) をアクティブにできます。

5 ページの『IBM Security QRadar 製品の機能』
IBM Security QRadar 製品資料では、オフェンス、フロー、アセット、ヒストリカル相関などの機能について説明していますが、すべての QRadar 製品でこれらの機能を利用できるわけではありません。使用する製品によっては、説明されている一部の機能をデプロイメントで使用できない場合があります。各製品の機能を確認して、必要な情報を入手してください。

システム・ヘルス情報の表示

システム・ヘルス・ビューには、IBM Security QRadar ホストに関するシステム通知とヘルス情報が表示されます。

CPU やメモリーの使用率、ネットワークおよびディスクの読み取りと書き込み、EPS および FPM レートなどの情報を表示するには、「管理」タブの「システムの正常性」アイコンをクリックします。

- マウスをグラフ上に移動すると、そのグラフのメトリックに関する詳細情報が表示されます。
- グラフをダブルクリックすると、管理対象ホストの追加レポートが表示されます。

QRadar のコンポーネントのタイプ

デプロイメント環境に追加される各 IBM Security QRadar アプライアンスには、QRadar での管理対象ホストの振る舞いを指定する、構成可能なコンポーネントがあります。

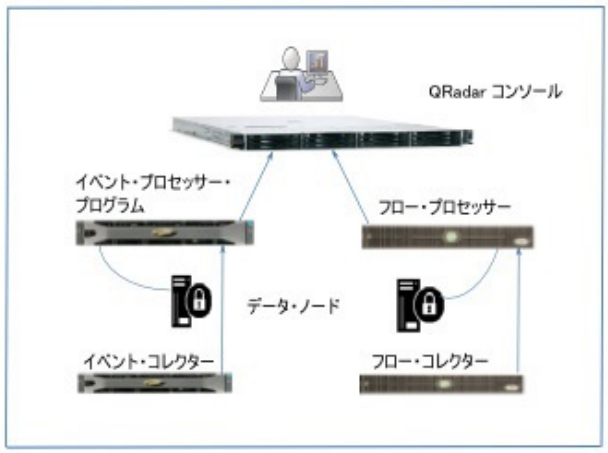


図 *1. QRadar* のイベントおよびフローのコンポーネント

QRadar コンソール

QRadar コンソールは、QRadar の製品インターフェース、リアルタイムのイベントおよびフローのビュー、レポート、オフェンス、アセット情報、および管理機能を提供します。分散環境では、QRadar コンソールを使用して、デプロイメント環境内の他のコンポーネントを管理します。

イベント・コレクター

イベント・コレクターはローカルおよびリモートのログ・ソースからイベントを収集し、生のイベント・データを正規化して、QRadar で使用できるようにします。システム・リソースを節約するために、イベント・コレクター は同一のイベントを 1 つにまとめて、イベント・プロセッサーにデータを送信します。

イベント・プロセッサー

イベント・プロセッサーは、1 つまたは複数の イベント・コレクター コンポーネントから収集されたイベントを処理します。コンソールで定義されているカスタム・ルールにイベントが一致した場合、イベント・プロセッサーは、ルール応答に定義されているアクションに従います。

各イベント・プロセッサーは、ローカル・ストレージを持っています。イベント・データはプロセッサーに保管されます。または、データ・ノードに保管できます。

QRadar QFlow コレクター

QRadar QFlow コレクター は、ネットワーク上のデバイスからネットワーク・フローを収集します。これには、ネットワーク・タップ、スパン・ポート、NetFlow、および QRadar フロー・ログなどのライブ・フィードや記録済みフィードが含まれます。

制約事項**:** QRadar Log Managerは、フロー収集をサポートしていません。

フロー・プロセッサー

フロー・プロセッサーは、1 つまたは複数の QRadar QFlow コレクター アプライアンスからのフローを処理します。フロー・プロセッサー アプライアンスは、ネットワーク内のルーターから外部ネットワーク・フロー (NetFlow、J-Flow、sFlow など) を直接収集することもできます。

フロー・プロセッサーには、オンボード・プロセッサーと、フロー・データの内部ストレージが含まれています。

データ・ノード

データ・ノードは、イベント・プロセッサーとフロー・プロセッサーから、セキュリティー・イベントとフローを受信し、データをディスクに保管します。

データ・ノードは、常にイベント・プロセッサーまたはフロー・プロセッサーに接続されています。

オフサイト・ソース・アプライアンスとオフサイト・ターゲット・アプライアンス

オフサイト・アプライアンスは、QRadar コンソール によってモニターされているデプロイメント環境の一部ではない QRadar アプライアンスです。

オフサイト・ソース・アプライアンスは、正規化されたデータをイベント・コレクターに転送します。転送前にデータを暗号化するように、オフサイト・ソースを構成することができます。

オフサイト・ターゲット・アプライアンスは、デプロイメント環境内の任意のイベント・コレクターまたは任意のプロセッサーから、正規化されたイベント・データまたはフロー・データを受信します。

新しいバージョンの QRadar システムは、それより古いバージョンの QRadar システムからのデータを受信できますが、古いバージョンは、それより新しいバージ

ョンからのデータを受信できません。問題を避けるために、送信側をアップグレードする前に、すべての受信側をアップグレードしてください。

データ・ノード

データ・ノードとは、ストレージ容量を増やし、検索のパフォーマンスを向上させるために、イベント・プロセッサーおよびフロー・プロセッサーに追加できるアプライアンスです。IBM Security QRadar デプロイメント環境に追加できるデータ・ノードの数に制限はなく、この追加はいつでも行うことができます。各データ・ノードは 1 つのプロセッサーにのみ接続できますが、1 つのプロセッサーは複数のデータ・ノードをサポートできます。

デプロイメントの計画について詳しくは、「*IBM Security QRadar* アーキテクチャーおよびデプロイメント・ガイド」を参照してください。

データ・ノードの追加後のデータのリバランス

データ・ノードを追加すると、検索およびシステム全体のパフォーマンスを向上させるために、IBM Security QRadar によってデータのリバランスが行われます。

データのリバランスでは、古いデータを圧縮解除したり、元のストレージ・デバイス上のデータを移動してすべての接続デバイスに均等に分散させるなどの処理を行います。

例えば、ご使用のデプロイメント環境のイベント・プロセッサーが受信する 1 秒当たりのイベント数 (EPS) が 20,000 であるとします。データ・ノードが追加されると、QRadar は自動的に、イベント・プロセッサーと、そのイベント・プロセッサーが利用できるすべてのデータ・ノードにイベントを分散します。3 つのデータ・ノードを追加した場合、イベント・プロセッサーは、5,000 EPS を保管し、接続されている各データ・ノードに 5,000 EPS を送信します。イベント・プロセッサーは依然としてすべてのイベントを処理しますが、データ・ノードによって追加のストレージ、索引付け、および検索の機能が提供され、全体的なパフォーマンスが向上します。

QRadar V7.2.6 以前で収集されたデータ

デフォルトでは、QRadar V7.2.6 以前のバージョンで収集されたデータは圧縮されません。データ圧縮は、デバイス上の使用可能なストレージがしきい値より低いことを QRadar が検出した場合にのみ行われます。データのボリュームがしきい値量に戻るまで、ディスク保守プロセスでデータが `gzip` フォーマットに圧縮され、データ削除ポリシーが適用されます。

データ・ノードを追加すると QRadar によってデータのリバランスが行われます。そして、十分なストレージ・スペースが使用可能になると、`gzip` フォーマットのデータが圧縮解除されます。古いデータの検索パフォーマンスはすぐに向上します。多くの検索では、圧縮解除された、より新しいデータが使用されるため、パフォーマンスは向上し続けます。

現在、V7.2.7 より前のデータは圧縮解除されているため、ディスク・ボリュームがフリー・ストレージ・スペースのしきい値をすぐに超えてしまう可能性があります。使用可能なディスク・スペースがしきい値設定を下回ると、フリー・ストレー

ジのしきい値に達するまでは、保存ポリシーに従って、ディスク保守プロセスによって、圧縮に適格なデータが圧縮されます。

QRadar V7.2.7 以降で収集されたデータ

QRadar V7.2.7 では、すべての新規データは圧縮フォーマットでディスクに書き込まれます。ディスク保守プロセスでは、新規データは圧縮されません。

データ削除ポリシーは、データ・フォーマットによる影響を受けません。QRadar が使用可能なストレージのしきい値を超えると、データ保存設定に従って、ディスク保守プロセスによって古いフォーマットと新しいフォーマットの両方のデータが削除されます。

データ・リバランスの進行状況の表示

データ・ノードを追加すると、IBM Security QRadar は自動的にデータを再配分し、デプロイメント環境内のストレージ・ボリューム全体でバランスを取るようにします。

検索のパフォーマンスが改善されるのは、データのリバランスが完了した後です。データ・リバランスの進行状況を表示することができ、さらにディスク・スペースの使用率などのデータも表示できます。

手順

1. 「管理」タブで、「システムおよびライセンス管理」アイコンをクリックします。
2. 「表示」リストで「システム」を選択します。
3. ホストの表で、詳細を表示する管理対象ホストを選択します。
   - 管理対象ホストのクラスターの情報を表示するには、最上位のホストを選択します。
   - 特定のデータ・ノードの情報を表示するには、そのデータ・ノードを選択します。
4. 「アクション」メニューで、「システムの表示と管理」をクリックします。
5. 「セキュリティー・データの分布」タブをクリックして、データ・リバランスの進行状況とデータ・ノード・アプライアンスの容量を表示します。

   注: データ・ノードのリバランスの進行状況に関する情報は、「管理」タブのデプロイメント・ステータス・バーでも確認できます。

すべてのイベント・データのデータ・ノード・アプライアンスへの保存

イベント・プロセッサーのパフォーマンスを改善するには、IBM Security QRadar がすべてのイベント・データをデータ・ノード・アプライアンスに保存するように構成します。この構成では、イベント・プロセッサーはイベントの処理のみを実行します。イベント・プロセッサーはイベント・データをローカルに保管しません。

イベントの処理のみを実行するように構成されたイベント・プロセッサーも、アクティブなデータ・ノード・アプライアンスが使用可能でない場合はローカルにデー

タを保存します。データ・ノード・アプライアンスが使用可能になると、QRadar は、可能な限り多くのデータをイベント・プロセッサーからデータ・ノードに転送します。

手順

1. 「管理」タブで、「システムおよびライセンス管理」アイコンをクリックします。
2. 「表示」リストで「システム」を選択します。
3. ホスト表でイベント・プロセッサーを選択し、「デプロイメント・アクション」メニューで「ホストの編集」をクリックします。
4. 「コンポーネント管理」設定アイコン ( ) をクリックします。
5. 「イベント・プロセッサー」の下の「イベント・プロセッサー・モード」フィールドで、「処理のみ」を選択します。
6. 「保存」をクリックし、再度「保存」をクリックします。
7. 「管理」タブで、「変更のデプロイ」をクリックします。

データ・ノードのコンテンツのアーカイブ

着信データの保管に影響を与えずにデータ・ノードでヒストリカル・データへのオンライン・アクセスを提供するには、「アーカイブ」モードを使用するようにデータ・ノード・アプライアンスを構成します。

「アーカイブ」モードでは、アプライアンスは新規データを受信しませんが、既存データは保存されます。

手順

1. 「管理」タブで、「システムおよびライセンス管理」アイコンをクリックします。
2. 「表示」リストで「システム」を選択します。
3. ホスト表でデータ・ノード・アプライアンスを選択し、「デプロイメント・アクション」メニューで「ホストの編集」をクリックします。
4. 「コンポーネント管理」設定アイコン ( ) をクリックします。
5. 「データ・ノード・モード」フィールドで、「アーカイブ」を選択し、「保存」をクリックします。
6. 「管理」タブで、「変更のデプロイ」をクリックします。

次のタスク

データ・ノード・アプライアンスでのデータの保管を再開するには、モードを「アクティブ」に戻します。

ネットワーク・インターフェースの管理

デフォルトの管理インターフェースに加えて、IBM Security QRadar アプライアンスにネットワーク・インターフェースを追加し、代替のネットワーク接続を提供できます。

追加のネットワーク・インターフェースは以下の目的に使用できます。

- 高可用性 (HA) ピア間の専用クロスオーバー接続を提供する。クロスオーバー接続の構成は HA のセットアップ時に行います。
- インバウンド・イベントまたは外部フロー・ソースに専用のデータ接続インターフェースを提供する。TCP ベースのデータ・ソースは、データ収集インターフェースと同じサブネット内になければなりません。
- バックアップ・ストレージ・システムおよびネットワーク・ストレージ・システムに接続する (iSCSI)。
- インターフェースを結合することにより、帯域幅を拡大し、耐障害性を高める。

ネットワーク・インターフェースの構成

ボンディングを使用して、2 つ以上のネットワーク・インターフェースを単一チャネルに結合することにより、IBM Security QRadar アプライアンスの使用可能帯域幅を増やします。

このタスクについて

ボンディング・オプションを含め、QRadar アプライアンスのネットワーク管理インターフェースは、セットアップ時の UNIX シェル・プロンプトでのみ構成されます。

QRadar コンソールでの管理インターフェースの構成は、管理対象ホストを追加する前に行ってください。

既存のスレーブ・インターフェースを結合することはできません。管理インターフェースは、シェル・プロンプトでのみ結合できます。クロスオーバーの結合は「高可用性」(HA) 構成画面から行えます。

手順

1. 「管理」タブをクリックします。
2. ナビゲーション・メニューで、「システム構成」をクリックします。
3. 「システムおよびライセンス管理」アイコンをクリックします。
4. 「表示」メニューから、「システム」をクリックします。
5. ネットワーク・インターフェースを構成するホストを選択します。
6. 「アクション」 > 「システムの表示と管理」をクリックし、「ネットワーク・インターフェース」タブをクリックします。
7. ネットワーク・インターフェースを編集するには、以下の手順を実行します。
   a. 編集するデバイスを選択し、「編集」をクリックします。
   b. 「ロール」リストから、以下のようにしてデバイスのロールを選択します。
      - デバイスをデータ収集に使用する場合は「通常」を選択します。このインターフェースには IP アドレスが必要です。

- デバイスがパケット収集に使用する IBM Security QRadar QFlow Collector の場合は、「モニター」を選択します。このインターフェースには IP アドレスは不要です。
- デバイスがネットワーク接続で使用されないようにする場合は、「無効」を選択します。

a. アクティブな HA ノードに構成を適用するには、「このインターフェース構成と **IP** アドレスをアクティブ **HA** ノードに適用する」をクリックします。

このオプションは、このシステムに HA を追加する場合にのみ使用されます。

b. 「保存」をクリックします。

8. 結合ネットワーク・インターフェースを作成するには、以下の手順を実行します。

「通常」または「モニター」のロールが割り当てられている 2 つ以上のインターフェースを結合できます。結合できるのは、同じロールが割り当てられているインターフェースのみです。

a. デバイスを選択し、「ボンディング」をクリックします。
b. IP アドレスとネットマスクを入力します。
c. アクティブな HA ノードに構成を適用するには、「このインターフェース構成と **IP** アドレスをアクティブ **HA** ノードに適用する」をクリックします。

注**:** このオプションを選択することにより、2 つの高可用性 (HA) ノードのうち、いずれかのアクティブなノードでインターフェースをアクティブに保つことができます。Syslog メッセージや NetFlow データ・レコードなどのインバウンド・データを受信するために使用するインターフェースでこのオプションを使用できます。このオプションにより、プライマリー・ノードとセカンダリー・ノード間で、アクティブなノードに対してデータがマイグレーションされます。

d. ボンディング・オプションを入力します。 このインターフェースに構成されているデフォルトのボンディング・オプションは、`mode=0 miimon=100` です。

ボンディング・モードに関する詳細の説明**:**

結合されたインターフェースでは、それらが接続されているスイッチの機能に応じてさまざまな動作モードがサポートされます。

次の表で、使用する可能性のあるボンディング・モードをいくつか説明します。

表 *11.* ボンディング・モード

ボンディング・モード	ボンディング名	説明
モード = 0	バランス・ラウンドロビン	パケットは、使用可能な最初のスレーブから最後のスレーブへと続く順序で送信されます。
モード = 1	アクティブ・バックアップ	アクティブなスレーブは 1 つのみです。アクティブ・スレーブで障害が発生すると、別のスレーブがアクティブになります。
モード = 2	バランス XOR	それぞれの宛先 MAC アドレスに同じスレーブが使用されます。
モード = 3	ブロードキャスト	すべてのデータをすべてのスレーブで送信します。
モード = 4	802.3ad	リンク集約制御プロトコル (LACP) を使用して、二重設定と速度を共有する集約グループを作成します。
モード = 5	バランス送信ロード・バランシング (TLB)	発信ネットワーク・データは、すべてのスレーブに分散されます。指定されたスレーブが着信トラフィックを受信し、そのトラフィックは、指定されたスレーブに障害が発生するとバックアップ・スレーブにフェイルオーバーされます。
モード = 6	バランス・アダプティブ・ロード・バランシング (ALB)	IPV4 ネットワーク・トラフィックの場合に、送信ロード・バランシング (TLB) と受信ロード・バランシング (RLB) の両方を含みます。

特定のボンディング・オプションの構成について詳しくは、ベンダー固有のオペレーティング・システムの資料を参照してください。

e. 「追加」をクリックし、スレーブとして追加するインターフェースを選択して、「**OK**」をクリックします。

f. 「保存」をクリックして、結合インターフェースを作成します。

9. 結合インターフェースを分解して単体のインターフェースに戻すには、結合されたデバイスを選択し、「ボンディング解除」をクリックします。

次のタスク

結合されたインターフェースの設定の構成時に接続が機能しない場合は、SSH を使用してホストにログインし、`/var/log/message` ログ・ファイルを調べて、ネットワーク・インターフェース・エラーがないかを確認してください。

または、設定を mode=1 に変更してみてください。あるいは、結合されたインターフェース・グループ内のイーサネット接続のうち 1 つを除いてすべてを物理的に切断してみてください。この回避策がうまく機能する場合、ご使用のスイッチ・インフラストラクチャーで、使用しようとしているモードがサポートされていることを確認してください。スイッチには mode=4 をサポートしないものがあります。

QRadar のシステム時刻

デプロイメント環境が複数のタイム・ゾーンにまたがる場合、IBM Security QRadar コンソールと同じタイム・ゾーンを使用するようにすべてのアプライアンスを構成します。あるいは、すべてのアプライアンスがグリニッジ標準時 (GMT) を使用するように構成できます。

QRadar ユーザー・インターフェースから IBM Security QRadar システム時刻を構成します。時刻は、手動で構成することも、システム時刻を保守するように Network Time Protocol (NTP) サーバーを構成する方法でも構成できます。

QRadar コンソールと管理対象ホストの間で時刻が自動的に同期されます。

タイム・ゾーンの不一致で発生する問題

検索とデータ関連機能を正しく動作させるには、すべてのアプライアンスの時刻設定を QRadar コンソール・アプライアンスと同期させる必要があります。タイム・ゾーン設定が一致しない場合、QRadar の検索とレポート・データの間に矛盾した結果が生じる可能性があります。

アキュムレーター・サービスは、ローカル・ストレージを持つすべてのアプライアンスで実行され、1 分ごとの集計、毎時および毎日のロールアップを作成します。QRadar は、時系列グラフとレポート内の集計データを使用します。分散デプロイメントでタイム・ゾーンが一致しない場合、集計データの集め方が原因で、AQL 照会の結果と比較した際にレポートと時系列グラフが矛盾した結果を示す可能性があります。

QRadar の検索は、Ariel データベースに保管されているデータに対して実行され、日付構造 (YYYY/MM/DD/HH/MM) を使用してファイルをディスクに保管します。データがディスクに書き込まれた後でタイム・ゾーンを変更すると、Ariel データベース内のファイル命名シーケンスが壊れてしまうため、データ保全性の問題が発生する可能性があります。

システム時刻の構成

QRadar コンソールで、時刻を手動で設定するか、NTP サーバーを使用して時刻を保守することで、システム時刻を構成します。QRadar は、QRadar コンソールの時刻を、デプロイメント内の管理対象ホストと同期します。

手順

1. 「管理」タブで、「システムおよびライセンス管理」アイコンをクリックします。
2. 「表示」リストで「システム」を選択します。
3. システム時刻設定の構成対象となるホストを選択します。
4. 「アクション」メニューから、「システムの表示と管理」をクリックします。
5. 「システム時刻」タブをクリックします。
6. QRadar コンソールで時刻を構成するには、次の手順に従います。
   a. 「タイム・ゾーン」リストで、QRadar コンソールに該当するタイム・ゾーンを選択します。

b. 時刻を手動で構成するには、「手動時刻設定」をクリックして、コンソールの日時を設定します。

注**:** システム時刻を夏時間調整 (DST) の変更による影響を受ける未来の日付に設定した場合、設定した時刻は 1 時間調整されます。例えば、米国で 2016 年 7 月 4 日に、日付を 2016 年 12 月 16 日に、時刻を午後 8:00 に設定したとします。設定した時刻は、DST の変更を無視して、午後 7:00 に調整されます。

c. NTP サーバーを使用して時刻を管理するには、次の手順に従います。

1) 「**NTP** サーバーを指定」をクリックし、「さらに追加」をクリックします。

2) 「サーバー **1** のアドレス」フィールドに、NTP サーバーの IP アドレスまたはホスト名を入力します。ホスト名は、DNS サーバーによって解決されます。

7. 管理対象ホストで時刻を構成するには、「タイム・ゾーン」リストでそのホストに該当するタイム・ゾーンを選択します。

管理対象ホストで構成できるのは、タイム・ゾーンのみです。システム時刻は QRadar コンソールと同期されますが、管理対象ホストが異なるタイム・ゾーンにある場合は、そのタイム・ゾーンに変更できます。

8. 「保存」をクリックします。

9. 「**OK**」をクリックして、サービスが再始動されることに同意するか、「キャンセル」をクリックして、変更をキャンセルします。

イベントおよびフローのデータ収集は、hostcontext サービスと tomcat サービスが再開されるまで停止します。

次のタスク

VMware システム上でシステム時刻を設定してからシステムを再始動すると、その変更は失われる可能性があります。時刻の変更が失われるのを防止するために、仮想マシンの構成ファイルを編集して、次の行を同期プロパティーに追加することで、仮想デバイスの同期を無効にできます。

```
tools.syncTime = "FALSE"
time.synchronize.continue = "FALSE"
time.synchronize.restore = "FALSE"
time.synchronize.resume.disk = "FALSE"
time.synchronize.shrink = "FALSE"
time.synchronize.tools.startup = "FALSE"
```

.vmx ファイルは、通常し、仮想マシンを作成したディレクトリーにあります。詳しくは、ベンダー固有のオペレーティング・システムの資料を参照してください。

NAT 対応ネットワーク

ネットワーク・アドレス変換 (NAT) は、あるネットワークの IP アドレスを別のネットワークの異なる IP アドレスに変換します。NAT では、変換プロセスを介して要求が管理され、内部 IP アドレスは非表示になるため、IBM Security QRadar デプロイメント環境のセキュリティーを強化できます。NAT を使用すると、専用の内部ネットワークに配置されているコンピューターは、ネットワーク・デバイス

(通常はファイアウォール) を通じて変換され、そのネットワークを介して公共のインターネットと通信できます。NAT を使用して、個々の内部 IP アドレスを個々の外部 IP アドレスにマップします。

QRadar の NAT 構成では、静的な NAT が必要です。また、許可されるパブリック IP アドレスは、管理対象ホストごとに 1 つのみです。

QRadar ホストがピアと同じ NAT グループに属していない、つまり別の NAT グループに属している場合、そのホストは、パブリック IP アドレスを使用して到達するように構成されます。例えば、QRadar コンソールでパブリック IP アドレスを構成する場合、同じ NAT グループに配置されているすべてのホストは、QRadar コンソールのプライベート IP アドレスを使用して通信します。異なる NAT グループに配置されている管理対象ホストは、QRadar コンソールのパブリック IP アドレスを使用して通信します。

外部変換を必要としないこれらの NAT グループ・ロケーションのいずれかにホストがある場合は、「プライベート **IP**」フィールドと「パブリック **IP**」フィールドの両方にプライベート IP アドレスを入力してください。コンソールとは異なる NAT グループを使用するリモート・ロケーション内のシステムでは、コンソールへの接続を確立できるようにする必要があるため、引き続き外部 IP アドレスと NAT が必要です。コンソールと同じ NAT グループに配置されているホストのみが、パブリック IP アドレスとプライベート IP アドレスに同じアドレスを使用できます。

NAT グループの構成

ネットワーク・アドレス変換 (NAT) グループを構成して、IBM Security QRadar 管理対象ホストがインターネットとの通信に必要とするパブリック IP アドレスの数を制限します。

始める前に

NAT 対応ネットワークが、静的 NAT 変換を使用していることを確認します。

このタスクについて

変更をデプロイする前に、デプロイメント内の管理対象ホストごとに NAT 構成を完了することが重要です。NAT 対応でない管理対象ホストは、デプロイメント後に QRadar コンソールと通信できなくなる場合があります。

各ネットワークで QRadar コンソールのパブリック IP アドレスが同じ場合、QRadar は、複数の NAT ネットワークをサポートできます。

手順

1. 「管理」タブで、「システムおよびライセンス管理」アイコンをクリックします。
2. 「表示」リストで「システム」を選択します。
3. QRadar コンソールで NAT グループを構成するには、次の手順に従います。
   a. ホスト表で、QRadar コンソール・アプライアンスを選択します。

b. 「デプロイメント・アクション」メニューで、「ホストの編集」をクリックします。
c. 「ネットワーク・アドレス変換」チェック・ボックスを選択します。
d. 「**NAT** グループ」リストで、コンソールが属する NAT グループを選択するか、「設定」アイコン () をクリックして、新しい NAT グループを作成します。
e. 「パブリック **IP**」フィールドに、コンソールのパブリック IP アドレスを入力し、「保存」をクリックします。

4. 同じネットワークの各管理対象ホストが、QRadar コンソールと同じ NAT グループを使用するように構成します。
a. ホスト表で、管理対象ホスト・アプライアンスを選択します。
b. 「デプロイメント・アクション」メニューで、「ホストの編集」をクリックします。
c. 「ネットワーク・アドレス変換」チェック・ボックスを選択します。
d. 「**NAT** グループ」リストで、QRadar コンソールが属する NAT グループを選択します。
e. 「パブリック **IP**」フィールドに、管理対象ホストのパブリック IP アドレスを入力します。

注**:** 管理対象ホストは、NAT を使用する管理対象ホストにイベント・コレクターが接続する場合を除き、同じパブリック IP アドレスとプライベート IP アドレスを使用するように構成します。

f. 「保存」をクリックします。

5. 「管理」タブ・メニューで、「拡張」 > 「すべての構成のデプロイ」をクリックします。

完全構成をデプロイすると、QRadar によりすべてのサービスが再始動されます。イベントおよびフローに関するデータ収集は、デプロイが完了するまで停止します。

次のタスク

QRadar コンソールと、デプロイメント後に NAT 対応にならないホストとの間の通信の問題を修正するには、管理対象ホストの iptables ルールを編集して、QRadar コンソールによる管理対象ホストへのアクセスを許可するようにローカルのファイアウォールを構成します。

管理対象ホストの NAT 状況の変更

ネットワーク・アドレス変換 (NAT) を使用するように管理対象ホストを構成して、同一ネットワーク内の QRadar コンソールおよび他の管理対象ホストと確実に通信できるようにします。

始める前に

NAT 対応ネットワークが、静的 NAT 変換を使用していることを確認します。

同じネットワーク内の QRadar コンソールおよびすべての管理対象ホストは、同じ NAT グループのメンバーである必要があります。

管理対象ホストの NAT 状況を変更するには、デバイスを更新する前に、IBM Security QRadar 内で管理対象ホストの構成を必ず更新します。構成を先に更新しておくことにより、ホストが到達不能になることが回避され、そのホストへの変更のデプロイを確実に続行できます。

手順

1. 「管理」タブで、「システムおよびライセンス管理」アイコンをクリックします。
2. 「表示」リストで「システム」を選択します。
3. ホスト表でホストを選択し、「デプロイメント・アクション」メニューで「ホストの編集」をクリックします。
4. NAT を無効にするには、「ネットワーク・アドレス変換」チェック・ボックスをクリアします。
5. NAT を有効にするには、以下の手順に従います。
   a. 「ネットワーク・アドレス変換」チェック・ボックスを選択します。
   b. 「**NAT** グループ」リストから、管理対象ホストが属するグループを選択します。
   c. 「パブリック **IP**」フィールドに、管理対象ホストが別の NAT グループ内の他のホストと通信するために使用するパブリック IP アドレスを入力します。
6. 「保存」をクリックします。
7. 「管理」タブ・メニューで、「拡張」 > 「すべての構成のデプロイ」をクリックします。

   完全構成をデプロイすると、QRadar によりすべてのサービスが再始動されます。イベントおよびフローに関するデータ収集は、デプロイが完了するまで停止します。

次のタスク

NAT を有効にした場合、通信する管理対象ホスト用にファイアウォール構成を更新する必要が生じる場合があります。詳しくは、 79 ページの『ローカル・ファイアウォールの構成』を参照してください。

オフサイト・ホストの管理

オフサイト・ホストとは、デプロイメント環境の QRadar コンソールを介してアクセスできない QRadar アプライアンスです。QRadar デプロイメント環境との間でデータの転送と受信を行うようにオフサイト・ホストを構成できます。

オフサイト・ソースの構成

イベントおよびフロー・データを別のデプロイメント内のイベント・コレクターに転送するには、オフサイト・ソースを含めるようにターゲット・デプロイメントを構成して、送信元のコンピューターを判別できるようにします。

このタスクについて

接続エラーを回避するため、オフサイト・ソースとオフサイト・ターゲットのコンポーネントを構成する際は、オフサイト・ソースのある IBM Security QRadar コンソールを先にデプロイします。それから、オフサイト・ターゲットのある QRadar コンソールをデプロイします。

手順

1. 「管理」タブで、「システムおよびライセンス管理」アイコンをクリックします。
2. 「表示」リストで「システム」を選択します。
3. 「デプロイメント・アクション」メニューで、「オフサイト・ソースの管理」をクリックします。
4. 「追加」をクリックし、パラメーターを構成します。

   名前には最大 20 文字を使用でき、下線およびハイフンを含めることができます。
5. 「保存」をクリックします。
6. 「接続の管理」をクリックし、どの QRadar ホストのデータを受信するかを指定します。

   このホストには、データを受信するために イベント・コレクター が必要です。
7. この手順を繰り返して、すべてのオフサイト・ソースを構成します。
8. 変更をデプロイします。

オフサイト・ターゲットの構成

イベントおよびフロー・データを別のデプロイメント内のイベント・コレクターに転送するには、オフサイト・ターゲットを含めるようにソース・デプロイメントを構成して、データの送信先のコンピューターを判別できるようにします。

始める前に

オフサイトのターゲット・アプライアンスの listen ポートを把握しておく必要があります。デフォルトでは、イベントの listen ポートは 32004、フロー用のポートは 32000 です。

ターゲット・アプライアンスの listen ポートを調べるには、以下の手順を実行します。

1. ターゲット・デプロイメントで、「システムおよびライセンス管理」アイコンをクリックします。
2. ホストを選択し、「デプロイメント・アクション」 > 「ホストの編集」をクリックします。
3. 「コンポーネント管理」設定アイコン () をクリックし、「イベント転送 **listen** ポート」フィールドと「フロー転送 **listen** ポート」フィールドでポートを確認します。

このタスクについて

接続エラーを回避するため、オフサイト・ソースとオフサイト・ターゲットのコンポーネントを構成する際は、オフサイト・ソースのある IBM Security QRadar コンソールを先にデプロイします。それから、オフサイト・ターゲットのある QRadar コンソールをデプロイします。

手順

1. 「管理」タブで、「システムおよびライセンス管理」アイコンをクリックします。
2. 「表示」リストで「システム」を選択します。
3. 「デプロイメント・アクション」メニューで、「オフサイト・ターゲットの管理」をクリックします。
4. 「追加」をクリックし、パラメーターを構成します。

   名前には最大 20 文字を使用でき、下線およびハイフンを含めることができます。

   イベントを listen するデフォルト・ポートは 32004、フロー用のポートは 32000 です。
5. 「保存」をクリックします。
6. 「接続の管理」をクリックし、どの QRadar ホストのデータを受信するかを指定します。

   イベント・コレクターが存在するホストのみがリストに表示されます。
7. この手順を繰り返して、すべてのオフサイト・ターゲットを構成します。
8. 変更をデプロイします。

QRadar 製品の公開鍵の生成

IBM Security QRadar で正規化イベントを転送するには、公開鍵ファイル `/root/.ssh/id_rsa.pub`, を、オフサイト・ソースからオフサイト・ターゲットにコピーする必要があります。

オフサイト・ソースとオフサイト・ターゲットが別々のシステム上にある場合は、公開鍵が自動的に生成されます。オフサイト・ソースとオフサイト・ターゲットの両方が 1 つのオールインワン・システム上にある場合は、公開鍵は自動的には生成されません。手動で公開鍵を生成する必要があります。

手順

公開鍵を手動で生成するには、以下の手順を実行します。

1. SSH を使用して、root ユーザーとしてシステムにログインします。
2. 公開鍵を生成するには、以下のコマンドを入力します。

   ```
   opt/qradar/bin/ssh-key-generating
   ```
3. Enter を押します。

公開鍵と秘密鍵のペアが生成され、/root/.ssh/id_rsa フォルダーに保存されます。

フィルターに掛けられたフローの転送

フィルターに掛けられたフローの転送をセットアップできます。フィルターに掛けられたフローを使用して、複数のボックス間でフロー転送を分割し、特定の調査用に特定のフローを転送することができます。

手順

1. ターゲット・システムで、ソース・システムをオフサイト・ソースとしてセットアップします。
   a. 「管理」タブで、「システムおよびライセンス管理」 > 「デプロイメント・アクション」 > 「オフサイト・ソースの管理」をクリックします。
   b. ソース・システムの IP アドレスを追加し、「イベントの受信」または「フローの受信」(あるいはその両方) を選択します。
   c. 「接続の管理」を選択し、オフサイト接続の受信を予期するホストを選択します。
   d. 「保存」をクリックします。
   e. 変更内容を有効にするには、「拡張」」メニューから「すべての構成のデプロイ」」を選択します。
2. ソース・システムで、宛先転送、IP アドレス、およびポート番号をセットアップします。
   a. 「メインメニュー」 > 「管理」をクリックします。
   b. 「宛先転送」 > 「追加」をクリックします。
   c. ターゲット・システムの IP アドレスと、宛先ポートを設定します。
   d. ソース・システムのポート番号に対して 32000 と入力します。ポート 32000 はフロー転送に使用されます。
   e. 「イベント・フォーマット」リストから「正規化済み」を選択します。
3. ルーティング・ルールをセットアップします。
   a. 「メインメニュー」 > 「管理」をクリックします。
   b. 「ルーティング・ルール」 > 「追加」をクリックします。
   c. 追加するルールを選択します。

      注**:** ルールはオフェンスに基づいてフローを正確に転送するだけです。あるいは、「ルーティング・ルール」画面で「オフライン転送 **(Offline Forwarding)**」が選択されている場合、CRE 情報に基づいてフローを転送します。

   「ルーティング・ルール」画面でフィルターに掛けられたフローが転送されます。

例**:** 正規化されたイベントとフローの転送

正規化されたイベントとフローを転送するには、データの送信元コンピューターをターゲット・デプロイメントが把握できるように、オフサイト・ソースを含めてタ

ーゲット・デプロイメントを構成します。データの送信先コンピューターをソース・デプロイメントが把握できるように、オフサイト・ターゲットを含めてソース・デプロイメントを構成します。

このタスクについて

デプロイメント間でのイベント・データとフロー・データの転送を次の図に示します。

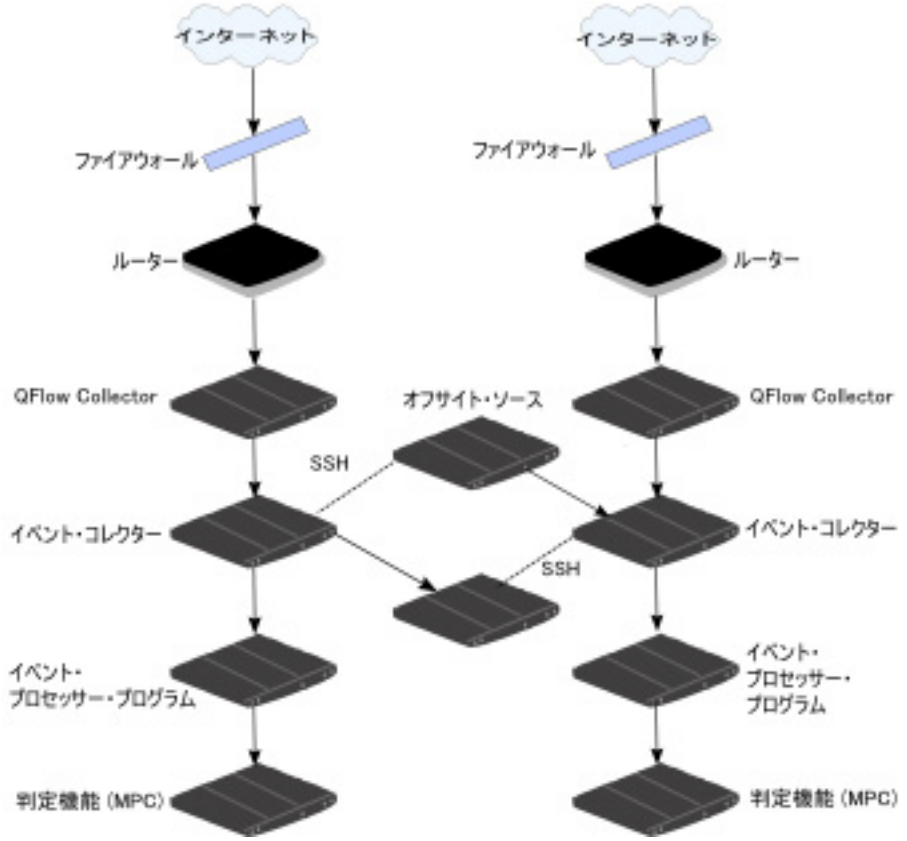


図 *2. SSH* を使用したデプロイメント間のデータの転送

オフサイト・ソースまたはターゲットがオールインワン・システムである場合、公開鍵は自動的には生成されないため、公開鍵を手動で生成する必要があります。詳しくは、 70 ページの『QRadar 製品の公開鍵の生成』を参照してください。

手順

デプロイメント A からデプロイメント B に正規化されたイベントとフローを転送するには、次の手順を実行します。

1. デプロイメント A でオフサイト・ターゲットを構成します。

   オフサイト・ターゲットの構成には、データを受信する、デプロイメント B のイベント・コレクターの IP アドレスが含まれます。
2. デプロイメント A でオフサイト・ソースを構成します。

オフサイト・ソースの構成には、データを送信する、デプロイメント A のイベント・コレクターの IP アドレスとポート番号が含まれます。

3. 暗号化されたデータを転送するには、オフサイト・ソースとオフサイト・ターゲットの両方で暗号化を有効にする必要があります。

適切なアクセスを確実にするために、ソース・システム (デプロイメント A) の SSH 公開鍵をターゲット・システム (デプロイメント B) が使用できるようにする必要があります。例えば、デプロイメント A とデプロイメント B との間で暗号化有効にするには、次の手順に従います。

4. **ssh-keygen -1 -t rsa** コマンドを使用して SSH 鍵を作成し、ディレクトリーとパスフレーズについてのプロンプトが表示されたら、Enter を押します。

   デフォルトでは、id_rsa.pub ファイルは /root/.ssh ディレクトリーに格納されます。

5. ソース・システム (デプロイメント A) のイベント・コレクターと QRadar コンソールの /root/.ssh ディレクトリーに id_rsa.pub ファイルをコピーします。

6. ファイル名を authorized_keys に変更します。

ターゲット・システムにイベント・データとフロー・データを送信する適切な権限付きで、ソース・システムが構成されていることを確認します。

7. **chmod 600 authorized_keys** コマンドを使用して **rw** 所有者特権をこのファイルと親ディレクトリーに割り当てていない場合、**-i** パラメーターを指定して **ssh-copy-id** コマンドを使用することで、使用する ID ファイル /root/.ssh/id_rsa.pub を指定してください。

   例えば、エントリーを追加するか、ターゲット・コンソールに適切な特権付きで新しい authorized_keys ファイルを作成するには、次のコマンドを入力します。このコマンドでは、重複エントリーの検査は行われません。

   ```
   ssh-copy-id -i root@10.100.133.80
   ```

8. イベントとフローの転送に対して、他の構成アクティビティー (いずれかのコンソールへの管理対象ホストの追加など) による割り込みが発生しないように、ソース・システムを構成します。

   例えば、イベントを転送するコンソールに管理対象ホストを追加する場合、管理対象ホストの /root/.ssh ディレクトリーに authorized_keys ファイルが存在している必要があります。存在しないと、管理対象ホストの追加に失敗します。管理対象ホストとコンソールとの間で暗号化を使用するかどうかに関係なく、このファイルは必要です。

9. ソース・システム (デプロイメント A) の QRadar コンソールで、/opt/qradar/conf の下に ssh_keys_created ファイルを作成します。

10. ファイルが適切にバックアップおよびリストアされるように、所有者とグループを「**nobody**」に、権限を「**775**」に変更します。

    ```
    chown nobody:nobody /opt/qradar/conf/ssh_keys_created
    chmod 775 /opt/qradar/conf/ssh_keys_created
    ```

11. 接続エラーを防止するために、ソース・システム (デプロイメント A) に変更をデプロイする前に、ターゲット・システム (デプロイメント B) に変更をデプロイしてください。

次のタスク

イベント・コレクターの構成またはモニター・ポートを更新する場合、オフサイト・ソースとオフサイト・ターゲットの構成を手動で更新して、デプロイメント間の接続を維持する必要があります。

ソース・システム (デプロイメント A) を切断する場合、両方のデプロイメントから接続を削除する必要があります。ソース・システム (デプロイメント A) からオフサイト・ターゲットを削除し、次にターゲット・システム (デプロイメント B) からオフサイト・ソースを削除します。

管理対象ホスト

データ収集とイベントおよびフローの処理の柔軟性を向上させるために、コレクター、プロセッサー、データ・ノードなどのコンソール以外の管理対象ホストを追加することで、分散 IBM Security QRadar デプロイメント環境を構築します。

QRadar 環境の計画および構築について詳しくは、「*IBM Security QRadar* アーキテクチャーおよびデプロイメント・ガイド」を参照してください。

ソフトウェア互換性要件

デプロイメント環境内のすべての IBM Security QRadar アプライアンスのソフトウェアのバージョンは、バージョンおよびフィックスパック・レベルが同じである必要があります。異なるバージョンのソフトウェアを使用するデプロイメントはサポートされません。これは、混合ソフトウェア環境では、ルールが起動されなかったり、オフェンスが作成および更新されなかったり、検索結果でエラーが発生したりするためです。

管理対象ホストで QRadar コンソールとは異なるソフトウェアのバージョンを使用している場合、既にそのホストに割り当て済みのコンポーネントを表示できる場合がありますが、そのコンポーネントを構成したり、新規コンポーネントの追加または割り当てを行ったりすることはできません。

管理対象ホストの帯域幅に関する考慮事項

状態および構成データを複製するには、IBM Security QRadar コンソールとすべての管理対象ホストとの間に最低でも 100 Mbps の帯域幅を確保してください。ログ・アクティビティーとネットワーク・アクティビティーを検索する場合や 1 秒当たりのイベント数 (EPS) が 10,000 件を超える場合は、より多くの帯域幅が必要です。

データをイベント・プロセッサーにストア・アンド・フォワードするように構成されたイベント・コレクターは、設定したスケジュールに従ってデータを転送します。収集されるデータ量に対応できる十分な帯域幅があることを確認してください。そうでない場合、転送元のアプライアンスはスケジュールされたペースを維持できません。

データ・センター間の帯域幅の制限は、以下の方法で緩和できます。

データをプライマリー・データ・センターで処理し、ホストに送信する
: コンソールが置かれているプライマリー・データ・センターでデータが収集

されたときにデータを処理し、ホストに送信するよう、ご使用のデプロイメントを設計してください。この設計の場合、すべてのユーザー・ベースの検索では、リモート・サイトからデータが送り返されるのを待つのではなく、ローカル・データ・センターからデータが照会されます。

QRadar 15XX の物理アプライアンスや仮想アプライアンスなどのストア・アンド・フォワード・イベント・コレクターをリモート・ロケーションにデプロイすると、ネットワーク内でのデータのバーストを制御できます。帯域幅はリモート・ロケーションで使用され、データの検索はリモート・ロケーションではなくプライマリー・データ・センターで行われます。

帯域幅が制限されている接続上でデータ量の多い検索を実行しない

帯域幅が制限されているリンク上でユーザーがデータ量の多い検索を実行しないようにしてください。検索で正確なフィルターを指定すると、リモート・ロケーションから取得するデータ量が抑制され、照会結果を戻すために必要となる帯域幅が削減されます。

暗号化

環境内の各アプライアンス間でセキュアなデータ転送が行われるように、IBM Security QRadar には、OpenSSH を使用する暗号化サポートが統合されています。暗号化は管理対象ホスト間で行われるため、暗号化を有効にするには、管理対象ホストが少なくとも 1 つ存在している必要があります。

暗号化が有効になっていると、接続を開始するクライアント上で、SSH プロトコル接続を使用してセキュア・トンネルが作成されます。管理対象ホストで暗号化を有効にした場合、その管理対象ホスト上のすべてのクライアント・アプリケーションに対して SSH トンネルが作成されます。非コンソール管理対象ホストで暗号化を有効にすると、データベースと、コンソールへの他のサポート・サービス接続に対して、暗号化トンネルが自動的に作成されます。

例えば、イベント・プロセッサーで暗号化を有効すると、イベント・プロセッサーとイベント・コレクターの間の接続、およびイベント・プロセッサーと判定機能の間の接続が暗号化されます。

管理対象ホストの追加

イベントおよびフロー・コレクター、イベントおよびフロー・プロセッサー、データ・ノードなどの管理対象ホストを追加して、データ収集およびデータ処理のアクティビティーを IBM Security QRadar デプロイメント全体に分散させます。

始める前に

管理対象ホストの IBM Security QRadar のバージョンおよびフィックスパック・レベルが、管理対象ホストを管理するために使用する QRadar コンソールと同じであることを確認してください。

管理対象ホストに対してネットワーク・アドレス変換 (NAT) を有効にするには、ネットワークで静的 NAT 変換を使用する必要があります。詳しくは、 65 ページの『NAT 対応ネットワーク』を参照してください。

このタスクについて

以下の表では、ユーザーが接続可能なコンポーネントについて説明しています。

表 *12.* サポートされるコンポーネント接続

ソース接続	ターゲット接続	説明
QRadar QFlow コレクター	イベント・コレクター	IBM Security QRadar QFlow Collector はイベント・コレクターにのみ接続できます。接続数は制限されません。 QRadar QFlow コレクター を 15xx アプライアンス上のイベント・コレクターに接続することはできません。
イベント・コレクター	イベント・プロセッサー	You can connect an イベント・コレクターは、1 つのイベント・プロセッサーにのみ接続できます。 非コンソール・イベント・コレクターを、同一システム上のイベント・プロセッサーに接続できます。 コンソール・イベント・コレクターは、コンソール・イベント・プロセッサーにのみ接続できます。この接続は削除できません。
イベント・プロセッサー	イベント・プロセッサー	コンソール・イベント・プロセッサーを、非コンソール・イベント・プロセッサーには接続できません。 非コンソール・イベント・プロセッサーを、別のコンソールまたは非コンソール・イベント・プロセッサーに接続できますが、同時に両方と接続することはできません。 非コンソール管理対象ホストを追加すると、非コンソール・イベント・プロセッサーがコンソール・イベント・プロセッサーに接続されます。
データ・ノード	イベント・プロセッサー	データ・ノードは、イベント・プロセッサーまたはフロー・プロセッサーにのみ接続できます。複数のデータ・ノードを同じプロセッサーに接続して、ストレージ・クラスターを作成することができます。
イベント・コレクター	オフサイト・ターゲット	接続数は制限されません。
オフサイト・ソース	イベント・コレクター	接続数は制限されません。 イベントのみのアプライアンスに接続されたイベント・コレクターは、「フローの受信」機能が有効なシステム・ハードウェアからオフサイト接続を受信できません。 QFlow のみのアプライアンスに接続されたイベント・コレクターは、「フローの受信」機能が有効になっているリモート・システムからオフサイト接続を受信できません。

デプロイメント環境で IBM Security QRadar Incident Forensics を構成した場合は、QRadar Incident Forensics 管理対象ホストを追加できます。詳しくは、「*IBM Security QRadar Incident Forensics* インストール・ガイド」を参照してください。

デプロイメント環境で IBM Security QRadar Vulnerability Manager を構成した場合は、脆弱性スキャナーと脆弱性プロセッサーを追加できます。詳しくは、「*IBM Security QRadar Vulnerability Manager* ユーザー・ガイド」を参照してください。

デプロイメント環境で IBM Security QRadar Risk Manager を構成した場合は、管理対象ホストを追加できます。詳しくは、「*IBM Security QRadar Risk Manager* インストール・ガイド」を参照してください。

手順

1. 「管理」タブで、「システムおよびライセンス管理」アイコンをクリックします。
2. 「表示」リストで「システム」を選択します。
3. 「デプロイメント・アクション」メニューで、「ホストの追加」をクリックします。
4. 管理対象ホストの設定を構成するために、固定 IP アドレスとアプライアンスのオペレーティング・システム・シェルにアクセスするためのルート・パスワードを指定します。
5. 「追加」をクリックします。
6. オプション: 「デプロイメント・アクション」 > 「デプロイメントの表示」メニューを使用して、視覚化したデプロイメント環境を表示します。視覚化したデプロイメント環境の `PNG` イメージまたは Microsoft Visio (2010) `VDX` ファイルをダウンロードできます。
7. 「管理」タブ・メニューで、「拡張」 > 「すべての構成のデプロイ」をクリックします。

   完全構成をデプロイすると、QRadar によりすべてのサービスが再始動されます。イベントおよびフローに関するデータ収集は、デプロイが完了するまで停止します。

関連タスク:

116 ページの『混合環境での IPv4 のみの管理対象ホストのインストール』
デフォルトでは、IBM Security QRadar 製品で、IPv6 と IPv4 の混合モードのコンソールに IPv4 のみの管理対象ホストを追加することはできません。IPv4 のみの管理対象ホストを有効にするスクリプトを実行する必要があります。

管理対象ホストの構成

管理対象ホストを構成して、デプロイメント内で管理対象ホストが遂行するロールを指定します。例えば、コレクター、プロセッサー、またはデータ・ノードとして管理対象ホストを構成できます。暗号化設定の変更と、ネットワーク・アドレス変換 (NAT) グループへのホストの割り当ても実行できます。

QRadar デプロイメントのインストール後に、QRadar コンソールや管理対象ホスト・システムのネットワーク構成の変更 (IP アドレスの変更など) を行う場合は、

qchange_netsetup ユーティリティーを使用します。ネットワーク設定について詳しくは、製品の「インストール・ガイド」を参照してください。

始める前に

管理対象ホストの IBM Security QRadar のバージョンとフィックスパック・レベルが、それを管理するために使用する QRadar コンソールと同じであることを確認します。異なるバージョンの QRadar を使用する管理対象ホストの編集や削除はできません。

管理対象ホストに対してネットワーク・アドレス変換 (NAT) を有効にするには、ネットワークで静的 NAT 変換を使用する必要があります。詳しくは、 65 ページの『NAT 対応ネットワーク』を参照してください。

手順

1. 「管理」タブで、「システムおよびライセンス管理」アイコンをクリックします。
2. 「表示」リストで「システム」を選択します。
3. ホスト表でホストを選択し、「デプロイメント・アクション」メニューで「ホストの編集」をクリックします。
   a. 管理対象ホストのポート 22 に SSH 暗号化トンネルを作成するには、「ホスト接続の暗号化」チェック・ボックスを選択します。
   b. NAT 対応ネットワークを使用するように管理対象ホストを構成するには、「ネットワーク・アドレス変換」チェック・ボックスを選択し、「**NAT** グループ」と「パブリック **IP**」アドレスを構成します。
   c. 管理対象ホスト上のコンポーネントを構成するには、「コンポーネント管理」設定アイコン () をクリックし、オプションを構成します。
   d. 「保存」をクリックします。
4. 「管理」タブ・メニューで、「拡張」 > 「すべての構成のデプロイ」をクリックします。

   完全構成をデプロイすると、QRadar によりすべてのサービスが再始動されます。イベントおよびフローに関するデータ収集は、デプロイが完了するまで停止します。

関連タスク:

313 ページの『ストア・アンド・フォワード・スケジュールの作成』
ストア・アンド・フォワード・スケジュール・ウィザードを使用して、イベント・コレクターがイベント・プロセッサーへのデータ転送の開始と停止を行うタイミングを制御するスケジュールを作成します。

管理対象ホストの削除

デプロイメントから非コンソール管理対象ホストを削除できます。IBM Security QRadar コンソールをホストする管理対象ホストを削除することはできません。

始める前に

管理対象ホストの IBM Security QRadar のバージョンとフィックスパック・レベルが、それを管理するために使用する QRadar コンソールと同じであることを確認します。異なるバージョンの QRadar を実行しているホストを削除することはできません。

手順

1. 「管理」タブで、「システムおよびライセンス管理」アイコンをクリックします。
2. 「表示」リストで「システム」を選択します。
3. 「デプロイメント・アクション」メニューで、「ホストの削除」をクリックし、「**OK**」をクリックします。

   QRadar コンソール・ホストを削除することはできません。
4. 「管理」タブ・メニューで、「拡張」 > 「すべての構成のデプロイ」をクリックします。

   完全構成をデプロイすると、QRadar によりすべてのサービスが再始動されます。イベントおよびフローに関するデータ収集は、デプロイが完了するまで停止します。

ローカル・ファイアウォールの構成

ネットワーク外部の特定のデバイスから IBM Security QRadar 管理対象ホストへのアクセスを管理するには、ローカル・ファイアウォールを使用します。ファイアウォール・リストが空の場合、管理対象ホストへのアクセスは、デフォルトで開いているポートを除き、無効になります。

手順

1. 「管理」タブで、「システムおよびライセンス管理」アイコンをクリックします。
2. 「表示」リストで「システム」を選択します。
3. ファイアウォール・アクセス設定の構成対象となるホストを選択します。
4. 「アクション」メニューから、「システムの表示と管理」をクリックします。
5. 「ファイアウォール」タブをクリックし、ホストに接続する必要があるデバイスの情報を入力します。
   a. このホストに接続する必要があるデプロイメント外部のデバイスに対して、アクセスを構成します。
   b. このアクセス・ルールを追加します。
6. 「保存」をクリックします。

   QFlow 構成で**外部フロー・ソース・モニター・ポート**のパラメーターを変更する場合、ファイアウォール・アクセス構成も更新する必要があります。

E メールの構成

E メール・サーバーを構成して、IBM Security QRadar でアラート、レポート、通知、およびイベント・メッセージを配信します。

このタスクについて

QRadar をセットアップするときに、E メール・メッセージを送信するために使用するメール・リレー・サーバーが検索されます。

メール・サーバー設定を `localhost` と構成した場合、メール・メッセージは QRadar のボックスから送信されることはありません。

手順

1. 「管理」タブで、「システムおよびライセンス管理」アイコンをクリックします。
2. 「表示」リストで「システム」を選択します。
3. E メール設定の構成対象となるホストを選択します。
4. 「アクション」メニューから、「システムの表示と管理」をクリックします。
5. 「**E** メール・サーバー」タブをクリックし、使用する E メール・サーバーのホスト名または IP アドレスを入力します。

   QRadar が提供する E メール・サーバーを使用する場合は、ローカル E メール処理を使用するために `localhost` と入力します。
6. 「保存」をクリックします。

変更のデプロイ

「管理」タブから、構成設定を更新することができます。行った変更は、変更を手動でデプロイするまでは、それを格納するステージング・エリアに保存されます。

このタスクについて

「管理」タブにアクセスするか、管理用タスクを実行するたびに、QRadar は、デプロイされていない変更を検査します。デプロイされていない変更が検出されると、QRadar は、バナーを更新して詳細情報を表示します。変更を行うには、構成をデプロイする必要があります。

手順

1. 「管理」タブで、バナーを確認して、デプロイする必要がある構成の変更を検索します。
2. 「詳細の表示」をクリックして、デプロイされていない構成の変更に関する情報を確認します。
3. 次からデプロイメント方法を選択します。
   a. 現在のセッションでの変更のみをデプロイするには、「管理」タブ・バナーの「変更のデプロイ」をクリックします。
   b. 最後のデプロイ以降に行われたすべての構成の変更をデプロイするには、「拡張」 > 「すべての構成のデプロイ」をクリックします。

完全構成をデプロイすると、QRadar によりすべてのサービスが再始動されます。イベントおよびフローに関するデータ収集は、デプロイが完了するまで停止します。

タスクの結果

変更をデプロイすると、デプロイされていない変更のリストがバナーからクリアされ、デプロイされていない新しい変更がないかどうかが、ステージング領域で再度検査されます。

システムのシャットダウン

システムをシャットダウンすると、アプライアンスの電源が切れます。システムをシャットダウンする間は、IBM Security QRadar インターフェースが使用できなくなり、データ収集が停止します。

手順

1. 「管理」タブで、「システムおよびライセンス管理」アイコンをクリックします。
2. 「表示」リストで「システム」を選択します。
3. シャットダウンするシステムを選択します。
4. 「アクション」メニューから、「システムのシャットダウン」を選択します。

システムの再始動

システムを再始動すると、その間は、IBM Security QRadar インターフェースが使用できなくなり、データ収集が停止します。

手順

1. 「管理」タブで、「システムおよびライセンス管理」アイコンをクリックします。
2. 「表示」リストで「システム」を選択します。
3. 再始動するシステムを選択します。
4. 「アクション」メニューから、「システムの再始動」を選択します。

ログ・ファイルの収集

IBM Security QRadar ログ・ファイルには、デプロイメントに関する詳細情報 (ホスト名、IP アドレス、E メール・アドレスなど) が含まれています。トラブルシューティングにあたって支援が必要な場合は、ログ・ファイルを収集して IBM サポートに送信できます。

このタスクについて

1 つ以上のホスト・システムのログ・ファイルを同時に収集できます。デプロイメントのサイズと管理対象ホストの数によっては、この処理にはしばらく時間がかかります。QRadar コンソール・ログ・ファイルは各ログ・ファイル収集に自動的に含まれます。

ログ・ファイル・コレクションの実行中も引き続き QRadar コンソールを使用できます。システムがアクティブにログ・ファイルを収集している場合は、新しい収集要求を開始できません。アクティブな収集プロセスをキャンセルしてから新しい収集を開始してください。

ログ・ファイル収集プロセスが完了すると、「システム・モニター」ダッシュボードにシステム通知が表示されます。

手順

1. 「管理」タブで、「システムおよびライセンス管理」アイコンをクリックします。
2. 「表示」リストで「システム」を選択します。
3. ホスト表のホストを選択します。
4. 「アクション」 > 「ログ・ファイルの収集」をクリックします。
5. 「詳細オプション」をクリックし、ログ・ファイル収集のオプションを選択します。

   暗号化されたログ・ファイル・コレクションを暗号化解除できるのは、IBM サポートのみです。ログ・ファイル収集にアクセスする場合には、ファイルを暗号化しないでください。
6. 「ログ・ファイルの収集」をクリックします。

   「システム・サポート・アクティビティー・メッセージ」に、収集プロセスのステータスを示すメッセージが表示されます。
7. ログ・ファイル・コレクションをダウンロードするには、「ログ・ファイルの収集が正常に完了しました」の通知を待ってから、「ファイルをダウンロードするには、ここをクリックしてください」をクリックします。

QRadar コンソールでのルート・パスワードの変更

適切なセキュリティー対策として、QRadar コンソールのルート・パスワードを定期的に変更してください。

手順

1. SSH を使用して、root ユーザーとして QRadar コンソールにログインします。
2. root ユーザーのユーザー名とパスワードを入力します。

   ユーザー名とパスワードは、大/小文字が区別されます。
3. **passwd** コマンドを使用してパスワードを変更します。

SIM のリセット

デプロイメントの調整後に、SIM をリセットして、データベースとディスクからすべてのオフェンスと、送信元と宛先の IP アドレスを削除することで、追加のフォールス・ポジティブ情報の受信を回避します。

このタスクについて

ご使用のシステム内のデータ量によっては、SIM のリセット・プロセスに数分かかる場合があります。SIM のリセット・プロセス中に、IBM Security QRadar ユーザー・インターフェースの他の領域に移動しようとすると、エラー・メッセージが表示されます。

手順

1. 「管理」タブをクリックします。
2. 「拡張」メニューで、「**SIM** モデルのクリーンアップ」を選択します。
3. 「SIM データ・モデルのリセット」ウィンドウに表示された情報を確認します。
4. 次のいずれかのオプションを選択します。

オプション	説明
ソフト・クリーン	データベース内のすべてのオフェンスをクローズします。「ソフト・クリーン」オプションを選択した場合は、「すべてのオフェンスを非アクティブにする」チェック・ボックスも選択できます。
ハード・クリーン	現在およびヒストリカルのすべての SIM データ (オフェンス、送信元 IP アドレス、および宛先 IP アドレスを含む) がパージされます。

5. 続行する場合は、「データ・モデルをリセットしますか**?**」チェック・ボックスを選択します。
6. 「次へ進む」をクリックします。
7. SIM のリセット・プロセスが完了したら、「閉じる」をクリックします。
8. Web ブラウザーを最新表示します。

第 6 章 QRadarのセットアップ

「管理」タブの機能を使用して、IBM Security QRadar SIEMをセットアップします。

ネットワーク階層、自動更新、システム設定、イベントとフローの保存バケット、システム通知、コンソール設定、オフェンスのクローズ理由、索引管理を構成することができます。

関連概念:

5 ページの『IBM Security QRadar 製品の機能』
IBM Security QRadar 製品資料では、オフェンス、フロー、アセット、ヒストリカル相関などの機能について説明していますが、すべての QRadar 製品でこれらの機能を利用できるわけではありません。使用する製品によっては、説明されている一部の機能をデプロイメントで使用できない場合があります。各製品の機能を確認して、必要な情報を入手してください。

ネットワーク階層

IBM Security QRadar は、ネットワーク階層のオブジェクトおよびグループを使用して、ネットワーク・アクティビティーを表示したり、ネットワーク内のグループやサービスをモニターします。

ネットワーク階層の作成時に、ネットワーク・アクティビティーを確認するための最も効果的な方法を考慮してください。ネットワーク階層は、ネットワークの物理的なデプロイメントに似ている必要はありません。QRadar は、一定の範囲の IP アドレスによって定義可能なネットワーク階層をサポートしています。ネットワークは、さまざまな変数 (地理的な単位や事業単位など) に基づいて作成できます。

関連概念:

273 ページの『マルチテナント・デプロイメントでのネットワーク階層の更新』
「ネットワーク階層の定義」権限を持つテナント管理者は、自身のテナント内のネットワーク階層を変更できます。

ネットワーク階層を定義する際のガイドライン

IBM Security QRadar でネットワーク階層を構築することは、デプロイメント環境の構成に不可欠な最初のステップです。ネットワーク階層が適切に構成されていないと、QRadar はフローの向きを判断できません。また、信頼できるアセット・データベースを構築することも、便利なルールのビルディング・ブロックを利用することもできません。

ネットワーク階層を定義する際は、以下のガイドラインを考慮してください。

- システムおよびネットワークを、ロールまたは類似のトラフィック・パターン別に編成します。

  例えば、メール・サーバー、部門ユーザー、ラボ、開発チームのグループを含むネットワークを編成します。このような編成を使用することにより、ネットワー

クの振る舞いを区別したり、振る舞いに基づくネットワーク管理セキュリティー・ポリシーを施行したりすることができます。ただし、特有の振る舞いをするサーバーを、ネットワーク上の他のサーバーと一緒にグループ化しないでください。固有のサーバーを単独で配置することにより、QRadar 内でそのサーバーの可視性が高まり、そのサーバーに対する具体的なセキュリティー・ポリシーを作成するのが容易になります。

- トラフィック量が多いサーバー (メール・サーバーなど) をグループの最上位に配置します。このような階層にすることにより、矛盾が生じた場合でも視覚的に見分けやすくなります。
- オブジェクトが 15 個を超えるようなネットワーク・グループを構成しないでください。

  大規模ネットワーク・グループでは、各オブジェクトの詳細情報を参照するのが困難になる場合があります。デプロイメント環境で 600,000 を超えるフローを処理する場合は、複数の最上位グループを作成することを検討してください。
- 複数のクラスレス・ドメイン間ルーティング (CIDR) またはサブネットを単一のネットワーク・グループに結合して、ディスク・スペースを節約します。

  例えば、重要なサーバーを個別オブジェクトとして追加し、他の主要な関連サーバーを複数の CIDR オブジェクトにグループ化します。

表 *13.* 単一ネットワーク・グループ内の複数の *CIDR* およびサブネットの例

グループ	説明	**IP** アドレス
1	マーケティング	10.10.5.0/24
2	販売	10.10.8.0/21
3	データベース・クラスター	10.10.1.3/32 10.10.1.4/32 10.10.1.5/32

- 新規ネットワークを定義するときは、適切なポリシーおよび振る舞いモニターが適用されるように、1 つの包括的なグループを定義します。

  以下の例で、人事部門ネットワーク (10.10.50.0/24 など) を Cleveland グループに追加する場合、トラフィックは Cleveland ベースとして表示され、Cleveland グループに適用するすべてのルールがデフォルトで適用されます。

表 *14. 1* つの包括的グループの例

グループ	サブグループ	**IP** アドレス
Cleveland	Cleveland 各種	10.10.0.0/16
Cleveland	Cleveland 販売	10.10.8.0/21
Cleveland	Cleveland マーケティング	10.10.1.0/24

- ドメインが有効にされた環境では、各 IP アドレスが適切なドメインに割り当てられていることを確認します。

許容される CIDR 値

IBM Security QRadar は特定の CIDR 値を許容します。

以下の表に、QRadar が受け入れる CIDR 値のリストを示します。

表 15. 許容される *CIDR* 値

CIDR の長さ	マスク	ネットワークの数	ホスト数
/1	128.0.0.0	128 A	2,147,483,392
/2	192.0.0.0	64 A	1,073,741,696
/3	224.0.0.0	32 A	536,870,848
/4	240.0.0.0	16 A	268,435,424
/5	248.0.0.0	8 A	134,217,712
/6	252.0.0.0	4 A	67,108,856
/7	254.0.0.0	2 A	33,554,428
/8	255.0.0.0	1 A	16,777,214
/9	255.128.0.0	128 B	8,388,352
/10	255.192.0.0	64 B	4,194,176
/11	255.224.0.0	32 B	2,097,088
/12	255.240.0.0	16 B	1,048,544
/13	255.248.0.0	8 B	524,272
/14	255.252.0.0	4 B	262,136
/15	255.254.0.0	2 B	131,068
/16	255.255.0.0	1 B	65,534
/17	255.255.128.0	128 C	32,512
/18	255.255.192.0	64 C	16,256
/19	255.255.224.0	32 C	8,128
/20	255.255.240.0	16 C	4,064
/21	255.255.248.0	8 C	2,032
/22	255.255.252.0	4 C	1,016
/23	255.255.254.0	2 C	508
/24	255.255.255.0	1 C	254
/25	255.255.255.128	2 サブネット	124
/26	255.255.255.192	4 サブネット	62
/27	255.255.255.224	8 サブネット	30
/28	255.255.255.240	16 サブネット	14
/29	255.255.255.248	32 サブネット	6
/30	255.255.255.252	64 サブネット	2
/31	255.255.255.254	なし	なし
/32	255.255.255.255	1/256 C	1

例えば、接頭部境界に含まれるビット数がネットワークのナチュラル (またはクラスフル) マスクより少ない場合、ネットワークはスーパーネットと呼ばれます。接

頭部境界に含まれるビット数がネットワークのナチュラル・マスクより多い場合、ネットワークはサブネットと呼ばれます。

- 209.60.128.0 は、マスクが /24 のクラス C ネットワーク・アドレスです。
- 209.60.128.0 /22 は、以下を生成するスーパーネットです。
  - 209.60.128.0 /24
  - 209.60.129.0 /24
  - 209.60.130.0 /24
  - 209.60.131.0 /24
- 192.0.0.0 /25

  サブネット・ホストの範囲

  0 192.0.0.1-192.0.0.126

  1 192.0.0.129-192.0.0.254
- 192.0.0.0 /26

  サブネット・ホストの範囲

  0 192.0.0.1 - 192.0.0.62

  1 192.0.0.65 - 192.0.0.126

  2 192.0.0.129 - 192.0.0.190

  3 192.0.0.193 - 192.0.0.254
- 192.0.0.0 /27

  サブネット・ホストの範囲

  0 192.0.0.1 - 192.0.0.30

  1 192.0.0.33 - 192.0.0.62

  2 192.0.0.65 - 192.0.0.94

  3 192.0.0.97 - 192.0.0.126

  4 192.0.0.129 - 192.0.0.158

  5 192.0.0.161 - 192.0.0.190

  6 192.0.0.193 - 192.0.0.222

  7 192.0.0.225 - 192.0.0.254

関連タスク:

89 ページの『ネットワーク階層の定義』

IBM Security QRadar には、事前定義されたネットワーク・グループを含むデフォルトのネットワーク階層が含まれています。事前定義されたネットワーク階層オブジェクトを編集することも、新しいネットワーク・グループやオブジェクトを作成することもできます。

ネットワーク階層の定義

IBM Security QRadar には、事前定義されたネットワーク・グループを含むデフォルトのネットワーク階層が含まれています。事前定義されたネットワーク階層オブジェクトを編集することも、新しいネットワーク・グループやオブジェクトを作成することもできます。

このタスクについて

ネットワーク・オブジェクトは CIDR アドレスのコンテナーです。ネットワーク階層内の CIDR 範囲内にあるすべての IP アドレスは、ローカル・アドレスと解釈されます。ネットワーク・オブジェクトの CIDR 範囲内で定義されないすべての IP アドレスは、リモート IP アドレスと解釈されます。CIDR は 1 つのネットワーク・オブジェクトにのみ属しますが、CIDR 範囲のサブセットは別のネットワーク・オブジェクトに属することが可能です。ネットワーク・トラフィックは、最も正確な CIDR に一致します。ネットワーク・オブジェクトには複数の CIDR 範囲を割り当てることができます。

QRadar のデフォルトのビルディング・ブロックとルールの一部は、デフォルトのネットワーク階層オブジェクトを使用します。デフォルトのネットワーク階層オブジェクトを変更する前に、ルールとビルディング・ブロックを検索して、オブジェクトの用途と、オブジェクトの変更後に調整が必要になるルールとビルディング・ブロックを把握してください。誤ったオフェンスを防ぐために、ネットワーク階層、ルール、およびビルディング・ブロックを常に最新の状態に保持することが重要です。

手順

1. 「管理」タブで、「ネットワーク階層」アイコンをクリックします。
2. 「ネットワーク・ビュー (Network Views)」ウィンドウのメニュー・ツリーから、処理対象のネットワーク領域を選択します。
3. ネットワーク・オブジェクトを追加するには、以下の手順を実行します。
   a. 「追加」をクリックして、オブジェクトの固有の名前と説明を入力します。
   b. 「グループ」リストから、新規ネットワーク・オブジェクトを追加するグループを選択します。
   c. グループを追加するには、「グループ」リストの横にあるアイコンをクリックして、グループの名前を入力します。
   d. このオブジェクトの CIDR 範囲を入力し、「追加」をクリックします。
   e. 「作成」をクリックします。
   f. すべてのネットワーク・オブジェクトについて上記の手順を繰り返します。
4. 既存のネットワーク・オブジェクトを処理するには、「編集」または「削除」をクリックします。

関連概念:

87 ページの『許容される CIDR 値』
IBM Security QRadar は特定の CIDR 値を許容します。

自動更新

構成ファイルの更新を自動または手動で行い、最新のネットワーク・セキュリティー情報が構成ファイルに含まれるようにすることができます。

構成ファイルを更新することは、フォールス・ポジティブを除去し、最新の悪意のあるサイト、ボットネット、およびその他の疑わしいインターネット・アクティビティーからシステムを保護するのに役立ちます。

自動更新の要件

更新を受信するには、IBM Security QRadar コンソールをインターネットに接続する必要があります。コンソールがインターネットに接続されていない場合は、コンソールがファイルをダウンロードするための内部更新サーバーを構成する必要があります。

更新ファイルは IBM Fix Central (http://www.ibm.com/support/fixcentral) から手動でダウンロードできます。

現在の構成および情報の保全性を維持するために、既存の構成ファイルを置き換えるか、更新済みファイルを既存のファイルと統合します。

コンソールに更新をインストールして変更をデプロイすると、コンソールが管理対象ホストを更新します。

更新の説明

更新ファイルには、以下の更新が含まれている場合があります。

- コンテンツに基づく構成の更新。これには、構成ファイルの変更、脆弱性、QID マップ、サポート・スクリプト、およびセキュリティーの脅威情報の更新が含まれます。
- DSM、スキャナー、およびプロトコルの更新。構文解析の問題に対する訂正、スキャナーの変更、プロトコルの更新が含まれます。
- JAR ファイルの更新や大規模なパッチなど、ユーザー・インターフェース・サービスの再始動を必要とするメジャー更新。
- 日次の自動更新ログや QID マップ・スクリプトなど、ユーザー・インターフェース・サービスの再始動を必要としないマイナー更新。

高可用性デプロイメント用の自動更新

プライマリー・ホストで構成ファイルを更新し、変更をデプロイすると、セカンダリー・ホストで更新内容が自動的に反映されます。変更をデプロイしない場合、更新内容は毎時実行される自動プロセスによってセカンダリー・ホストに反映されます。

新規インストールおよびアップグレードの場合の自動更新の頻度

自動更新のデフォルトの頻度は、インストールのタイプと QRadar のバージョンによって決まります。

- V7.2 よりも前のバージョンの QRadar からアップグレードする場合は、更新頻度の設定値はアップデート後も変わりません。デフォルトでは更新は「毎週」に設定されますが、この頻度は手動で変更できます。
- QRadar V7.2 以降のバージョンを新規にインストールする場合は、更新のデフォルトの頻度は毎日です。頻度は手動で変更できます。

関連概念:

97 ページの『手動更新』
インターネットにアクセスできない IBM Security QRadar コンソールがデプロイメント環境に含まれている場合や、システムに対する更新を手動で管理する場合は、IBM Security QRadar 更新サーバーをセットアップすることで更新プロセスを手動で管理できます。

保留中の更新の表示

システムでは、週次の自動更新が事前構成されています。保留中の更新を「更新 (Updates)」ウィンドウで表示できます。

このタスクについて

システムは、週次更新を取得するのに十分な長さの期間運用されている必要があります。「更新 (Updates)」ウィンドウに更新が表示されない場合は、システムの運用期間がまだ週次更新が行われるほどの長さに達していないか、または更新が発行されていません。この場合は、新規更新を手動で確認できます。新規更新の確認について詳しくは、 95 ページの『新規更新の確認』を参照してください。

「更新の確認」ツールバーには、以下の機能があります。

表 16. 「更新の確認」ツールバーの機能

機能	説明
非表示 **(Hide)**	1 つ以上の更新を選択して「非表示 **(Hide)**」をクリックし、選択した更新を「更新の確認」ページから除去します。非表示にされた更新は、「非表示更新の復元 (Restore Hidden Updates)」ページで表示および復元することができます。詳しくは、 96 ページの『非表示更新の復元』を参照してください。
インストール **(Install)**	更新は、手動でインストールすることができます。更新を手動でインストールすると、インストール・プロセスが 1 分以内に開始します。詳しくは、 96 ページの『自動更新の手動インストール』を参照してください。
スケジュール **(Schedule)**	選択した更新をコンソールで手動インストールする特定の日時を構成できます。スケジューリングは、オフピーク時に更新のインストールをスケジュールする場合に役立ちます。詳しくは、 94 ページの『更新のスケジュール』を参照してください。

表 16. 「更新の確認」ツールバーの機能 (続き)

機能	説明
スケジュール解除	コンソールで更新を手動インストールするための事前構成スケジュールを削除できます。詳しくは、 94 ページの『更新のスケジュール』を参照してください。
名前で検索 **(Search By Name)**	特定の更新を名前で見つけることができます。
次の最新表示 **(Next Refresh)**	このカウンターは、次の自動最新表示までの時間を表示します。「更新の確認」ページの更新のリストは、60 秒ごとに自動的に最新表示されます。1 つ以上の更新を選択すると、タイマーは自動的に一時停止します。
一時停止 **(Pause)**	自動最新表示プロセスを一時停止します。自動最新表示を再開するには、「プレイ **(Play)**」をクリックします。
最新表示 **(Refresh)**	更新のリストを最新表示します。

手順

1. 「管理」タブをクリックします。
2. ナビゲーション・メニューで、「システム構成」をクリックします。
3. 「自動更新」をクリックします。
4. 更新の詳細を表示するには、更新を選択します。

自動更新設定の構成

自動更新設定をカスタマイズして、頻度、更新タイプ、サーバー構成、およびバックアップ設定を変更します。

このタスクについて

「自動デプロイ」を選択すると、自動的に更新をデプロイすることができます。「自動デプロイ」が選択されていない場合は、更新のインストール後に、「ダッシュボード」タブから変更を手動でデプロイする必要があります。

制約事項**:** 高可用性 (HA) 環境では、セカンダリー・ホストがアクティブである場合は自動更新はインストールされません。更新がインストールされるのは、プライマリー・ホストがアクティブ・ノードになった後です。

「サービスの自動再始動」を選択して自動更新を可能にすることはできますが、これにはユーザー・インターフェースを再始動することが必要になります。サービスが再始動すると、ユーザー・インターフェースが中断されます。代わりに、「更新の確認」ウィンドウから、更新を手動でインストールできます。

手順

1. 「管理」タブをクリックします。
2. ナビゲーション・メニューで、「システム構成」をクリックします。
3. 「自動更新」をクリックします。

4. ナビゲーション・メニューで、「設定の変更」をクリックします。
5. 「基本」タブで、更新のスケジュールを選択します。
6. 「構成の更新」セクションで、構成ファイルを更新するのに使用する方式を選択します。
   - カスタム・シグニチャー、カスタム・エントリー、およびリモート・ネットワークの構成に影響を与えることなく、既存の構成ファイルとサーバーの更新をマージするには、「自動統合」オプションを選択します。
   - カスタマイズをサーバー設定でオーバーライドするには、「自動更新」オプションを選択します。
7. 「**DSM**、スキャナー、プロトコルの更新」セクションで、更新をインストールするためのオプションを選択します。
8. 「メジャー更新」セクションで、新規リリースのメジャー更新を受信するオプションを選択します。
9. 「マイナー更新」セクションで、マイナーなシステムの問題に対するパッチを受信するオプションを選択します。
10. 次のオプションのいずれかを選択してください。
    - 更新のインストール後に更新の変更を自動的にデプロイする場合は、「自動デプロイ」チェック・ボックスを選択します。
    - 更新のインストール後にユーザー・インターフェース・サービスを自動的に再始動する場合は、「サービスの自動再始動」チェック・ボックスを選択します。
11. 「拡張」タブをクリックします。
12. 「**Web** サーバー」フィールドで、更新を取得する Web サーバーを入力します。 デフォルトの Web サーバーは、 https://qmmunity.q1labs.com/ です。
13. 「ディレクトリー」フィールドで、Web サーバーが更新を保管するディレクトリーの場所を入力します。 デフォルトのディレクトリーは、`autoupdates/` です。
14. オプション: 「プロキシー・サーバー」フィールドで、プロキシー・サーバーの URL を入力します。 アプリケーション・サーバーがインターネットに接続するためにプロキシー・サーバーを使用する場合は、プロキシー・サーバーが必要です。
15. オプション: 「プロキシー・ユーザー名」フィールドで、プロキシー・サーバーのユーザー名を入力します。 認証済みプロキシーを使用している場合は、ユーザー名が必要です。
16. 「プロキシー・パスワード」フィールドで、プロキシー・サーバーのパスワードを入力します。 認証済みプロキシーを使用している場合は、パスワードが必要です。
17. 更新に関するフィードバックを IBM に送信する場合は、「フィードバックの送信」チェック・ボックスを選択します。 更新中にエラーが発生する場合、フィードバックは Web フォームにより自動的に送信されます。

18. 「バックアップ保存期間」リストで、更新プロセス中に置換されたファイルを保管する日数を入力するか選択します。 ファイルは、「バックアップの場所」パラメーターで指定されている場所に保管されます。最短の期間は 1 日で、最長の期間は 65535 年です。
19. 「バックアップの場所」フィールドで、バックアップ・ファイルを保管する場所を入力します。
20. 「ダウンロード・パス」フィールドで、DSM の更新、マイナー更新、およびメジャー更新を保管するディレクトリー・パスの場所を入力します。 デフォルトのディレクトリー・パスは、/store/configservices/staging/updates です。
21. 「保存」をクリックします。

SSL または TLS インターセプトを使用するプロキシー・サーバーの背後での更新の構成

プロキシー・サーバーの背後で IBM Security QRadar の更新を構成するには、プロキシー・サーバーの CA 証明書を ca-bundle.crt ファイルに追加します。

手順

1. QRadar の ca-bundle.crt ファイルのバックアップ・コピーを作成します。例えば、コピー・コマンド cp /etc/ssl/certs/ca-bundle.crt{,bak} を使用して .bak ファイルを作成します。
2. プロキシー・サーバーからルート CA 証明書を取得します。詳しくは、プロキシー・サーバーの資料を参照してください。

   注: プロキシー・サーバーからのルート CA 証明書のみを使用する必要があります。
3. 以下のコマンドを 1 行で入力して、ca-bundle.crt ファイルに CA 証明書を追加します。

   ```
   openssl x509 -text -in /path/to/proxycert.crt >>
   /etc/pki/ca-trust/source/anchors/ca-bundle.qrdr.pem
   ```
4. 以下のコマンドを入力して証明書を抽出します。

   ```
   update-ca-trust extract
   ```

更新のスケジュール

自動更新は、「構成の更新」ページでの設定に従って、繰り返しスケジュールで発生します。また、特定の時刻に実行される更新または更新のセットをスケジュールすることもできます。

このタスクについて

システムに対するパフォーマンスの影響が少なくなるよう、大規模な更新はオフピーク時に実行Tするようスケジュールしてください。

各更新の詳細情報については、更新を選択してください。説明とエラー・メッセージが、ウィンドウの右ペインに表示されます。

手順

1. 「管理」タブをクリックします。
2. ナビゲーション・メニューで、「システム構成」をクリックします。
3. 「自動更新」をクリックします。
4. オプション: 特定の更新をスケジュールする場合は、スケジュールする更新を選択します。
5. 「スケジュール **(Schedule)**」リスト・ボックスから、スケジュールする更新のタイプを選択します。
6. カレンダーを使用して、スケジュール済み更新を開始する日時を選択します。

スケジュール済み更新のクリア

いずれのスケジュール済み更新も、取り消すことができます。

このタスクについて

スケジュール済み更新の状況は、「状況」フィールドに「スケジュール済み」と表示されます。スケジュールをクリアすると、更新の状況は「新規」と表示されます。

手順

1. 「管理」タブをクリックします。
2. ナビゲーション・メニューで、「システム構成」をクリックします。
3. 「自動更新」をクリックします。
4. ナビゲーション・メニューで、「更新の確認」をクリックします。
5. オプション: 特定のスケジュール済み更新をクリアする場合は、クリアする更新を選択します。
6. 「スケジュール解除」リスト・ボックスから、クリアするスケジュール済み更新のタイプを選択します。

新規更新の確認

IBM は定期的に更新を提供します。デフォルトで、自動更新機能は、更新を自動的にダウンロードしてインストールするようにスケジュールされています。事前構成スケジュール以外の時間に更新が必要な場合は、新規更新をダウンロードできます。

手順

1. 「管理」タブをクリックします。
2. ナビゲーション・メニューで、「システム構成」をクリックします。
3. 「自動更新」をクリックします。
4. ナビゲーション・メニューで、「更新の確認」をクリックします。
5. 「新規更新の取得 **(Get new updates)**」をクリックします。

自動更新の手動インストール

IBM は、定期的に更新を提供します。デフォルトでは、更新はご使用のシステムに自動的にダウンロードされ、インストールされます。ただし、事前構成スケジュール以外の時間に更新をインストールことは可能です。

このタスクについて

システムは、IBM Fix Central (www.ibm.com/support/fixcentral/) から新規更新を取得します。これには長時間かかる可能性があります。完了すると、新規更新が「更新 (Updates)」ウィンドウにリストされます。

手順

1. 「管理」タブをクリックします。
2. ナビゲーション・メニューで、「システム構成」をクリックします。
3. 「自動更新」をクリックします。
4. ナビゲーション・メニューで、「更新の確認」をクリックします。
5. オプション: 特定の更新をインストールする場合は、スケジュールする更新を選択します。
6. 「インストール **(Install)**」リスト・ボックスから、インストールする更新のタイプを選択します。

更新履歴の表示

更新が正常にインストールされるか、インストールに失敗すると、その更新は、「更新履歴の表示」ページに表示されます。

このタスクについて

更新の説明およびインストール・エラー・メッセージ (ある場合) が、「更新履歴の表示」ページの右ペインに表示されます。「更新履歴の表示」ページには、次の情報が表示されます。

手順

1. 「管理」タブをクリックします。
2. ナビゲーション・メニューで、「システム構成」をクリックします。
3. 「自動更新」をクリックします。
4. ナビゲーション・メニューで、「更新履歴の表示 **(View Update History)**」をクリックします。
5. オプション: 「名前で検索 **(Search by Name)**」テキスト・ボックスにキーワードを入力して Enter を押すと、特定の更新を名前で見つけることができます。
6. 特定の更新を調べるには、その更新を選択します。

非表示更新の復元

「更新の確認」ページから更新を削除できます。「非表示更新の復元」ページで非表示更新を表示および復元できます。

手順

1. 「管理」タブをクリックします。
2. ナビゲーション・メニューで、「システム構成」をクリックします。
3. 「自動更新」をクリックします。
4. ナビゲーション・メニューで、「非表示更新の復元 **(Restore Hidden Updates)**」をクリックします。
5. オプション: 更新を名前で見つけるには、「名前で検索 **(Search by Name)**」テキスト・ボックスにキーワードを入力して Enter を押します。
6. 復元する非表示更新を選択します。
7. 「リストア」をクリックします。

自動更新ログの表示

自動更新ログには、システムでの最新の自動更新が含まれています。

手順

1. 「管理」タブをクリックします。
2. ナビゲーション・メニューで、「システム構成」をクリックします。
3. 「自動更新」をクリックします。
4. ナビゲーション・メニューで、「ログの表示 **(View Log)**」をクリックします。

手動更新

インターネットにアクセスできない IBM Security QRadar コンソールがデプロイメント環境に含まれている場合や、システムに対する更新を手動で管理する場合は、IBM Security QRadar 更新サーバーをセットアップすることで更新プロセスを手動で管理できます。

自動更新パッケージには、各更新で必要なシステム構成ファイルに加えて、更新サーバーを手動でセットアップするために必要なすべてのファイルが含まれています。初期セットアップ後は、最新の自動更新パッケージをダウンロードして解凍するだけで、構成を手動で更新できます。

IBM Fix Central (www.ibm.com/support/fixcentral/) で通知を購読することにより、新しい更新の通知を受け取ることができます。

関連概念:

90 ページの『自動更新』
構成ファイルの更新を自動または手動で行い、最新のネットワーク・セキュリティー情報が構成ファイルに含まれるようにすることができます。

更新サーバーの構成

Apache サーバーを、IBM Security QRadar のデプロイメント環境用の更新サーバーとして構成します。

始める前に

Fix Central (www.ibm.com/support/fixcentral/) から自動更新パッケージをダウンロードします。QRadar 製品は、Security Systems の「製品グループ」で検索することができます。

手順

1. Apache サーバーにアクセスし、autoupdates/ という名前の更新ディレクトリーを作成します。

   デフォルトで、更新ディレクトリーは、Apache サーバーの Web ルート・ディレクトリーにあります。IBM Security QRadar の構成を変更して、このディレクトリーを別の場所に置くことができます。
2. オプション: 更新プロセスで使用する Apache ユーザー・アカウントおよびパスワードを作成します。
3. 自動更新パッケージ・ファイルを、Apache サーバーに作成した autoupdates/ ディレクトリーに保存します。
4. Apache サーバーで、次のコマンドを入力して、自動更新パッケージを解凍します。

   ```
   tar -zxf updatepackage-[timestamp].tgz
   ```
5. 「管理」タブで、「自動更新」アイコンをクリックします。
6. 「設定の変更」をクリックし、「拡張」タブをクリックします。
7. 「サーバー構成」ペインで、Apache サーバーの設定を構成します。
   a. 「**Web** サーバー」フィールドに、Apache サーバーのアドレスまたはディレクトリー・パスを入力します。

      Apache サーバーが標準外ポートで実行されている場合は、アドレスの末尾にポート番号を追加します。例えば、https://qmmunity.q1labs.com:8080/ と入力します。
   b. 「ディレクトリー」フィールドに、Web サーバーが更新情報を格納するディレクトリーの場所を入力します。

      デフォルトのディレクトリーは、autoupdates/ です。
   c. オプション: アプリケーション・サーバーがプロキシー・サーバーを使用してインターネットに接続する場合は、「プロキシー・サーバー」フィールドに URL を入力します。
   d. オプション: 認証プロキシーを使用する場合は、「プロキシー・ユーザー名」フィールドと「プロキシー・パスワード」フィールドに資格情報を入力します。
8. 「保存」をクリックします。
9. 「管理」タブで、「変更のデプロイ」をクリックします。
10. SSH を使用して、root ユーザーとして QRadar にログインします。
11. 次のコマンドを入力して、Apache サーバーに設定したユーザー名を構成します。

    ```
    /opt/qradar/bin/UpdateConfs.pl -change_username <username>
    ```

12. 次のコマンドを入力して、Apache サーバーに設定したパスワードを構成します。

    ```
    /opt/qradar/bin/UpdateConfs.pl -change_password <password>
    ```

13. 更新サーバーをテストするには、コマンド・ライン・インターフェースで、以下のコマンドを 1 行で入力します。

    ```
    wget -q -O- --no-check-certificate
    https://<your update server>/<directory path to updates>/manifest_list
    ```

14. ユーザー名とパスワードを入力します。

更新サーバーとしての QRadar コンソールの構成

ご使用の IBM Security QRadar コンソールを更新サーバーにするよう構成できます。

このタスクについて

ご使用の QRadar コンソールを更新サーバーにするよう構成するには、以下の 3 つのタスクを実行します。

- 自動更新ディレクトリーを作成します。
- IBM Fix Central から自動更新パッケージをダウンロードします。
- 自動更新を受け入れるように IBM Security QRadar を構成します。

手順

1. root ユーザーとして QRadar にログインします。
2. 以下のコマンドを入力して、自動更新ディレクトリーを作成します。

   ```
   mkdir /opt/qradar/www/autoupdates/
   ```

3. Fix Central (www.ibm.com/support/fixcentral/) から自動更新パッケージをダウンロードします。

   Fix Central では、QRadar 製品は Security Systems の「プロダクト・グループ」リストで検索できます。

4. 自動更新パッケージ・ファイルを、Apache サーバーに作成した `autoupdates/` ディレクトリーに保存します。
5. QRadar コンソールで、以下のコマンドを入力して自動更新パッケージを解凍します。

   ```
   tar -zxf updatepackage-[timestamp].tgz
   ```

6. QRadar ユーザー・インターフェースにログインします。
7. 「管理」タブで、「自動更新」アイコンをクリックします。
8. 「設定の変更」をクリックし、「拡張」タブを選択します。
9. 「**Web** サーバー」フィールドで、`https://localhost/` と入力します。
10. 「保存」をクリックします。

更新サーバーへの更新のダウンロード

更新は、Fix Central から更新サーバーにダウンロードできます。

始める前に

更新サーバーから更新を受信するよう、更新サーバーを構成して IBM Security QRadar をセットアップする必要があります。

手順

1. 自動更新パッケージを IBM Fix Central (http://www.ibm.com/support/fixcentral/) からダウンロードします。

   Fix Central では、QRadar 製品は Security Systems の「プロダクト・グループ」リストで検索できます。
2. 自動更新パッケージ・ファイルを、更新サーバーに作成した autoupdates/ ディレクトリーに保存します。
3. 以下のコマンドを入力して、自動更新パッケージを解凍します。

   ```
   tar -zxf autoupdate-[timestamp].tgz
   ```
4. root ユーザーとして QRadar にログインします。
5. 以下のコマンドを入力して、更新サーバーをテストします。

   ```
   lynx https://<your update server>/<directory path to updates>/manifest_list
   ```
6. 更新サーバーのユーザー名とパスワードを入力します。

システム設定の構成

共通のシステム設定は、「システム設定」ウィンドウで構成できます。

このタスクについて

「システム設定」ウィンドウには、以下のシステム設定の構成可能なパラメーターが表示されます。

- システム設定
- データベースの設定
- Ariel データベースの設定
- SNMP の設定
- 組み込み SNMP デーモンの設定
- アセット・プロファイルの設定
- コンソールの設定
- 認証の設定
- DNS の設定
- WINS の設定
- レポート作成の設定
- データ・エクスポートの設定

手順

1. 「管理」タブをクリックします。
2. ナビゲーション・メニューで、「システム構成」をクリックします。
3. 「システム設定」アイコンをクリックします。

4. システム設定を構成します。設定の説明を表示するには「ヘルプ」ボタンをクリックします。
5. 「保存」をクリックします。
6. 「管理」タブ・メニューで、「拡張」 > 「すべての構成のデプロイ」を選択します。

   完全構成をデプロイすると、QRadar によりすべてのサービスが再始動されます。イベントおよびフローに関するデータ収集は、デプロイが完了するまで停止します。

右クリック・メニューのカスタマイズ

機能に素早くアクセスできるようにするには、プラグイン・アプリケーション・プログラミング・インターフェース (API) を使用して、メニュー・オプションをカスタマイズします。例えば、NetBIOS をスキャンするオプションなどのメニュー項目をさらに追加することができます。

このタスクについて

ip_context_menu.xml ファイルで、右クリック・メニューをカスタマイズする menuEntry XML ノードを指定できます。

```
<menuEntry name="{Name}" description="{Description}" exec="{Command}"
url="{URL}" requiredCapabilities="{Required Capabilities}"/>
```

以下に、menuEntry エレメントに指定する各属性について説明します。

名前　右クリック・メニューに表示されるテキスト。

説明　項目の説明。説明のテキストは、メニュー・オプションのツールチップに表示されます。この説明はオプションです。

URL　新しいウィンドウで開く Web アドレスを指定します。

IP アドレスを表すために、プレースホルダー %IP% を使用できます。アンパーサンド文字 (&)、左不等号括弧 (<)、および右不等号括弧 (>) は、それぞれ &、<、および > というストリングを使用してエスケープする必要があります。

例えば、IP アドレス用のプレースホルダーが含まれる複数パラメーターの URL を渡すには、次の構文を使用できます。url="/lookup?&ip=%IP%;force=true"

コマンド

IBM Security QRadar コンソール上で実行するコマンド。コマンドの出力は、新しいウィンドウに表示されます。選択される IP アドレスを表すために、プレースホルダー %IP% を使用します。

必要な機能

このオプションを選択する前にユーザーが持っている必要がある「ADMIN」などの機能。コンマで区切って指定します。ここでリストしたすべての機能をユーザーが持っていない場合は、項目が表示されません。Required Capabilities はオプションのフィールドです。

編集したファイルは、以下の例に示すようになります。

```
<?xml version="1.0" encoding="UTF-8"?>
<!- This is a configuration file to add custom actions into
the IP address right-click menu. Entries must be of one of the
following formats: -->
<contextMenu>
<menuEntry name="Traceroute" exec="/usr/sbin/traceroute %IP%" />
<menuEntry name="External ARIN Lookup"
url="http://ws.arin.net/whois/?queryinput=%IP%" />
</contextMenu>
```

手順

1. SSH を使用して、root ユーザーとして IBM Security QRadar にログインします。
2. QRadar サーバー上で、/opt/qradar/conf/templates ディレクトリーにある ip_context_menu.xml ファイルを /opt/qradar/conf ディレクトリーにコピーします。
3. 編集のために /opt/qradar/conf/ip_context_menu.xml ファイルを開きます。
4. menuEntry エレメントの属性を編集します。
5. ファイルを保存して閉じます。
6. サービスを再始動するには、以下のコマンドを入力します。

```
systemctl restart tomcat
```

イベント列とフロー列の右クリック・メニューの拡張

「ログ・アクティビティー」テーブルまたは「ネットワーク・アクティビティー」テーブルの列で使用可能な右クリック・オプションに、他のアクションを追加できます。例えば、送信元 IP または宛先 IP に関する詳細情報を表示するためのオプションを追加できます。

イベントまたはフロー内にある任意のデータを、URL またはスクリプトに渡すことができます。

手順

1. SSH を使用して、root ユーザーとして QRadar コンソール・アプライアンスにログインします。
2. /opt/qradar/conf ディレクトリーに移動し、arielRightClick.properties という名前のファイルを作成します。
3. /opt/qradar/conf/arielRightClick.properties ファイルを編集します。以下の表を参照して、右クリック・メニューのオプションを決定するパラメーターを指定します。

表 *17. arielRightClick.properties* ファイルのパラメーターの説明

パラメーター	要件	説明	例
pluginActions	必須	URL またはスクリプト・アクションを示します。	

表 17. *arielRightClick.properties* ファイルのパラメーターの説明 (続き)

パラメーター	要件	説明	例
arielProperty	必須	右クリック・メニューを有効化する列 (Ariel フィールド名) を指定します。	**sourceIP** **sourcePort** **destinationIP** **qid**
text	必須	右クリック・メニューに表示されるテキストを指定します。	Google 検索
useFormattedValue	オプション	フォーマット済みの値をスクリプトに渡すかどうかを指定します。 username、payload などの属性のフォーマット済みの値が渡されるようにするには、true に設定します。フォーマット済みの値は、フォーマットされていない値に比べて、管理者が読み取りやすくなります。	イベント名 (QID) プロパティーに対してこのパラメーターが true に設定されている場合は、QID のイベント名がスクリプトに渡されます。 このパラメーターが false に設定されている場合は、未加工のフォーマットされていない QID 値がスクリプトに渡されます。
url	URL にアクセスする場合は必須	新規ウィンドウで開く URL と、その URL に渡すパラメーターを指定します。 $*Ariel_Field Name*$ というフォーマットを使用します。	sourceIPwebUrlAction.url= http://www.mywebsite.com? q=$sourceIP$
command	アクションがコマンドである場合は必須	コマンドまたはスクリプト・ファイルの絶対パスを指定します。	destinationPortScript Action.command=/bin/echo
arguments	アクションがコマンドである場合は必須	スクリプトに渡すデータを指定します。 $*Ariel_Field Name*$ というフォーマットを使用します。	destinationPortScript Action.arguments=qid

pluginActions リストで指定するキー名ごとに、*key name, property* というフォーマットのキーを使用してアクションを定義します。

4. ファイルを保存して閉じます。
5. QRadar ユーザー・インターフェースにログインします。
6. 「管理」タブをクリックします。
7. 「拡張」 > 「**Web** サーバーの再始動」を選択します。

例

以下の例は、送信元 IP アドレスの右クリック・オプションとして「*Test URL*」を追加する方法を示しています。

```
pluginActions=sourceIPwebUrlAction

sourceIPwebUrlAction.arielProperty=sourceIP
sourceIPwebUrlAction.text=Test URL
sourceIPwebUrlAction.url=http://www.mywebsite.com?q=$sourceIP$
```

以下の例は、宛先ポートに対してスクリプト・アクションを有効化する方法を示しています。

```
pluginActions=destinationPortScriptAction

destinationPortScriptAction.arielProperty=destinationPort
destinationPortScriptAction.text=Test Unformatted Command
destinationPortScriptAction.useFormattedValue=false
destinationPortScriptAction.command=/bin/echo
destinationPortScriptAction.arguments=$qid$
```

以下の例は、URL またはスクリプト・アクションにいくつかのパラメーターを追加する方法を示しています。

```
pluginActions=qidwebUrlAction,sourcePortScriptAction

qidwebUrlAction.arielProperty=qid,device,eventCount
qidwebUrlAction.text=Search on Google
qidwebUrlAction.url=http://www.google.com?q=$qid$-$device$-$eventCount$

sourcePortScriptAction.arielProperty=sourcePort
sourcePortScriptAction.text=Port Unformatted Command
sourcePortScriptAction.useFormattedValue=true
sourcePortScriptAction.command=/bin/echo
sourcePortScriptAction.arguments=$qid$-$sourcePort$-$device$-$CONTEXT$
```

アセットの保存値の概要

アセット・プロファイル情報を保管する期間 (日数) の追加情報。

- アセットは、一定の間隔で保存のしきい値に照らしてテストされます。デフォルトのクリーンアップ間隔は、12 時間です。
- 指定されたすべての保存期間は、情報の最終確認日 (情報が最後にスキャナーによって確認されたか、システムによってパッシブに監視されたかに関係なく) を基準とします。
- アセット情報は有効期限が切れると削除されます。つまり、クリーンアップ間隔の経過後に、保存しきい値内にあるすべてのアセット情報が保持されます。
- デフォルトでは、修正されていない脆弱性 (IBM Security QRadar Vulnerability Manager またはその他のスキャナーによって検出された脆弱性) に関連付けられているアセットは保持されます
- アセットは常に、ユーザー・インターフェースを使用して手動で削除することができます。

表 *18.* アセット・コンポーネント

アセット・コンポーネント	デフォルトの保存 (日数)	メモ
IP アドレス	120 日	デフォルトでは、ユーザー指定の IP アドレスは、手動で削除されるまで保持されます。

表 *18.* アセット・コンポーネント *(*続き*)*

アセット・コンポーネント	デフォルトの保存 **(**日数**)**	メモ
MAC アドレス (インターフェース)	120 日	デフォルトでは、ユーザー指定のインターフェースは、手動で削除されるまで保持されます。
DNS および NetBIOS のホスト名	120 日	デフォルトでは、ユーザー指定のホスト名は、手動で削除されるまで保持されます。

表 *18.* アセット・コンポーネント (続き)

アセット・コンポーネント	デフォルトの保存 (日数)	メモ
アセットのプロパティー	120 日	デフォルトでは、ユーザー指定の IP アドレスは、手動で削除されるまで保持されます。 この値が影響する可能性があるアセットのプロパティーは、「指定された名前」、「統一名」、「重み」、「説明」、「ビジネス・オーナー」、「ビジネスの連絡先 **(Business Contact)**」、「テクニカル・オーナー」、「技術担当者」、「ロケーション」、「検出信頼性 **(Detection Confidence)**」、「ワイヤレス **AP**」、「ワイヤレス **SSID**」、「スイッチ **ID**」、「スイッチ・ポート **ID**」、「**CVSS** 機密性要件 **(CVSS Confidentiality Requirement)**」、「**CVSS** 整合性要件 **(CVSS Integrity Requirement)**」、「**CVSS** 可用性要件 **(CVSS Availability Requirement)**」、「**CVSS** 二次的被害の可能性 **(CVSS Collateral Damage Potential)**」、「テクニカル・ユーザー」、「ユーザー指定 **OS (User Supplied OS)**」、「**OS** オーバーライド・タイプ **(OS Override Type)**」、「**OS** オーバーライド **ID (OS Override Id)**」、「拡張 **(Extended)**」、「レガシー **(7.2** 以前**) CVSS** リスク **(Legacy (Pre-7.2) Cvss Risk)**」、「**VLAN**」、および「アセット・タイプ **(Asset Type)**」です。

表 18. アセット・コンポーネント (続き)

アセット・コンポーネント	デフォルトの保存 (日数)	メモ
アセットの製品	120 日	デフォルトでは、ユーザー指定の製品は、手動で削除されるまで保持されます。 アセットの製品には、アセット OS、アセットのインストール済みアプリケーション、オープン・アセット・ポートに関連付けられた製品などがあります。
アセットの「開いている」ポート	120 日	
アセットの netBIOS グループ	120 日	NetBIOS グループはほとんど使用されることはなく、さらにお客様がその存在を意識しない場合があります。NetBIOS グループが使用されている場合は、120 日後に削除されます。
アセットのクライアント・アプリケーション	120 日	クライアント・アプリケーションは、まだユーザー・インターフェースでは利用されていません。この値は無視できます。
アセットのユーザー	30 日	

QRadar ログイン・メッセージ・ファイルの作成

IBM Security QRadar コンソールでログイン・メッセージを追加およびカスタマイズできます。

始める前に

ログイン・メッセージ・ファイルを作成するには、コマンド・ラインへの root アクセス権限が必要であり、Linux または UNIX でのファイル編集の経験も必要です。

手順

1. root ユーザーとして IBM Security QRadar にログインします。
2. `/etc/` ディレクトリーに移動します。
3. Linux または UNIX のテキスト・エディターで、ファイル名に特殊文字を使用せずにファイルを作成します。 例えば、`loginMSG` という名前のファイルを作成します。
4. メッセージを `loginMsg` ファイルに入力します。
5. メッセージを保存します。

6. ログイン・バナーを有効にするには、「管理」 > 「システム設定」に移動します。
7. 「認証設定」をクリックします。
8. 「ログイン・メッセージ・ファイル」フィールドに、次のファイル・パスを入力します。

   ```
   /etc/loginMsg
   ```
9. 「保存」をクリックします。
10. 「管理」タブ・メニューで、「変更のデプロイ」をクリックします。
11. QRadar からログアウトして、新しいログイン・メッセージを確認します。

IF-MAP サーバー証明書

Interface For Metadata Access Points (IF-MAP) ルールの応答は、IBM Security QRadar コンソールが、イベント、フロー、およびオフェンスから派生するアラートおよびオフェンスのデータを IF-MAP サーバーに公開できるようにします。

「システム設定」ウィンドウで IF-MAP 認証を構成するには、その前に、IF-MAP サーバー証明書を構成する必要があります。

基本認証用の IF-MAP サーバー証明書の構成

このタスクでは、 IF-MAP 証明書を基本認証用に構成する方法について説明します。

始める前に

IF-MAP サーバーの公開証明書のコピーを取得する方法については、IF-MAP サーバー管理者にお問い合わせください。証明書のファイル拡張子は `.cert` でなければなりません。

手順

1. SSH を使用して、root ユーザーとして IBM Security QRadar にログインします。
2. 証明書を `/opt/qradar/conf/trusted_certificates` ディレクトリーにコピーします。

相互認証用の IF-MAP サーバー証明書の構成

相互認証では、IBM Security QRadar コンソールと IF-MAP サーバーで証明書を構成する必要があります。

このタスクでは、QRadar コンソールでの証明書の構成手順について説明します。IF-MAP サーバーで証明書を構成する方法について詳しくは、IF-MAP サーバー管理者にお問い合わせください。

始める前に

IF-MAP サーバーの公開証明書のコピーを取得する方法については、IF-MAP サーバー管理者にお問い合わせください。証明書のファイル拡張子は .cert でなければなりません。

手順

1. SSH を使用して、root ユーザーとして IBM Security QRadar にログインします。
2. /opt/qradar/conf/trusted_certificates ディレクトリー内の証明書にアクセスします。
3. SSL 中間証明書と SSL Verisign ルート証明書を IF-MAP サーバーに CA 証明書としてコピーします。詳しくは、IF-MAP サーバー管理者にお問い合わせください。
4. 以下のコマンドを入力して、.pkcs12 ファイル拡張子を持つ PKCS (Public-Key Cryptography Standards) ファイルを作成します。

   ```
   openssl pkcs12 -export -inkey <private_key> -in <certificate> -out
   <pkcs12_filename.pkcs12> -name "IFMAP Client"
   ```

5. 以下のコマンドを入力して、pkcs12 ファイルを /opt/qradar/conf/key_certificates ディレクトリーにコピーします。

   ```
   cp <pkcs12_filename.pkcs12> /opt/qradar/conf/key_certificates
   ```

6. 証明書認証が行われる IF-MAP サーバーにクライアントを作成し、SSL 証明書をアップロードします。詳しくは、IF-MAP サーバー管理者にお問い合わせください。
7. 以下のコマンドを入力して、ディレクトリーのアクセス権を変更します。

   ```
   chmod 755 /opt/qradar/conf/trusted_certificates
   chmod 644 /opt/qradar/conf/trusted_certificates/*.cert
   ```

8. 以下のコマンドを入力して、Tomcat サービスを再始動します。

   ```
   systemctl restart tomcat
   ```

QRadar 製品での SSL 証明書の置き換え

デフォルトでは、IBM Security QRadar は、自己署名 Security Sockets Layer 証明書を使用して構成されます。自己署名証明書を使用して Web にアクセスすると、証明書を認識できないことを示す警告メッセージでプロンプトが出されます。この SSL 証明書は、更新された自己署名証明書、内部の認証局 (CA) が署名した証明書、またはパブリック CA が署名した証明書のいずれかで置き換えることができます。

SSL 証明書の概要

SSL は、通信のプライバシーを保護するセキュリティー・プロトコルです。これにより、クライアント/サーバー・アプリケーションは、盗聴、改ざん、メッセージの偽造を防ぐように設計された方法で通信することができます。

SSL は、オンライン・トランザクションを保護するために Web サイトで使用される業界標準です。Web サーバーは、SSL リンクを生成するために SSL 証明書を必

要とします。SSL 証明書は、内部の認証局または信頼できる第三者の認証局によって発行されます。

トラステッド・ルート

ブラウザーおよびオペレーティング・システムには、プリインストールされた、信頼できる証明書のリストが組み込まれています。これらの証明書は、トラステッド・ルート認証局ストアにインストールされています。

表 *19. QRadar* でサポートされる証明書

証明書	説明
自己署名	自己署名証明書を使用すると、基本的なセキュリティーが確保され、ユーザーとアプリケーションとの間でデータを暗号化できます。自己署名証明書は既存の既知のルート認証局では認証できないため、その不明な証明書に関する警告がユーザーに表示されます。続行するには、ユーザーはその証明書を受け入れる必要があります。
内部 CA 署名	内部のルート CA を独自に所有している組織は、その内部 CA を使用して証明書を作成できます。この証明書は、QRadar でサポートされており、内部のルート CA も QRadar 環境にインポートされます。
パブリック CA / 中間 CA 署名	QRadar では、既知のパブリック CA で署名された証明書と中間証明書がサポートされます。パブリック署名証明書は、QRadar で直接使用できます。また、中間 CA で署名された証明書は、その署名証明書と中間証明書の両方を使用してインストールされ、有効な証明書機能を提供します。 **注:** 中間証明書は、自社の環境で複数の SSL 鍵を作成し、それらの鍵を既知の/商用の証明書ベンダーによって署名されるようにする組織でよく使用されます。中間鍵を使用するときは、この中間鍵からサブ鍵を作成できます。この構成を使用するときは、中間証明書とホスト SSL 証明書の両方を使用して QRadar を構成し、ホストへの接続で証明書のパス全体を検証できるようにする必要があります。

QRadar コンポーネント間の SSL 接続

QRadar は、コンポーネント間のすべての内部 SSL 接続を確立する際に、QRadar コンソールにプリインストールされている Web サーバー証明書を使用します。プリインストールされている証明書を置き換えるときは、証明書のインストール・プロセスにより、デプロイメントのすべての管理対象ホスト (QRadar Incident Forensics アプライアンスを除く) に証明書がコピーされます。

QRadar の信頼できるすべての証明書が以下の要件を満たしている必要があります。

- 証明書が X.509 証明書であり、PEM Base64 エンコードが使用されている。
- 証明書のファイル拡張子が .cert、.crt、.pem、または .der である。
- 証明書を含む鍵ストア・ファイルの拡張子が .truststore である。
- 証明書ファイルが /opt/qradar/conf/trusted_certificates ディレクトリーに保管されている。

重要: IBM Security QRadar Incident Forensics を使用している場合は、お客様サポート (www.ibm.com/support/) に連絡し、QRadar Incident Forensics 鍵ストアにカスタム SSL 証明書をインストールする方法、または QRadar Incident Forensics 鍵ストア内のカスタム SSL 証明書を更新する方法を確認してください。

パスワードを使用して SSL 鍵を構成した場合は、サービスが再始動するたびに手動でパスワードを入力する必要があります。この構成では、QRadar パッチのインストール時、HA フェイルオーバー時、システム再始動時などにパスワードを入力するまで、Web UI サービスは使用できません。この場合、ユーザーはログインすることができず、QRadar の管理対象ホストは、Web サービスが使用可能になるまで、構成の更新を取得したり、ログ・ソース、ルール、およびデータ・ストレージの状況メッセージを報告したりできません。

2048 ビットの RSA 鍵を使用した SSL 証明書署名要求の作成

1. SSH を使用して、QRadar コンソールにログインします。
2. 以下のコマンドを使用して、秘密鍵ファイルを生成します。

   ```
   openssl genrsa -out qradar.key 2048
   ```

   注: 秘密暗号オプションは使用しないでください。互換性の問題が発生する場合があります。
   現行ディレクトリーに qradar.key ファイルが作成されます。このファイルは、証明書をインストールするときに使用するので、保持しておいてください。
3. 証明書署名要求 (CSR) ファイルを生成します。内部の CA または商用の認証局で SSL 証明書を作成するには、qradar.csr ファイルを使用します。以下のコマンドを実行し、プロンプトが表示されたら、必要な情報を入力します。

   ```
   openssl req -new -key qradar.key -out qradar.csr
   ```

   出力例:

   ```
   コマンド・ラインのプロンプトに従って以下の情報を入力します。
   [root@qradar ~]# openssl genrsa -out qradar.key 2048
   Generating RSA private key, 2048 bit long modulus
   ....................................+++
   ......................+++
   e is 65537 (0x10001)
   [root@bluecar ~]# openssl req -new -key qradar.key -out qradar.csr
   You are about to be asked to enter information that will be incorporated
   into your certificate request.
   What you are about to enter is what is called a Distinguished Name or a DN.
   There are quite a few fields but you can leave some blank
   For some fields there will be a default value,
   If you enter '.', the field will be left blank.
   -----
   Country Name (2 letter code) [XX]:US
   State or Province Name (full name) []:MyState
   ```

```
Locality Name (eg, city) [Default City]:MyCity
Organization Name (eg, company) [Default Company Ltd]:MyCompany
Organizational Unit Name (eg, section) []:MyCompanyOrg
Common Name (eg, your name or your server's hostname) []:qradar.mycompany.com
Email Address []:email@mycompany.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
[root@bluecar ~]#
```

4. CSR 内の情報を送信前に検証する場合は、以下のコマンドを入力します。

   ```
   openssl req -noout -text -in qradar.csr
   ```

   入力した情報に誤りがあった場合は、OpenSSL コマンドを実行し直して、CSR ファイルを再作成します。
5. セキュア・ファイル転送プロトコルまたは他のプログラムを使用して、CSR ファイルをご使用のコンピューターに安全にコピーします。
6. 署名のために、内部の認証局または商用の認証局に、その手順に従って CSR を送信します。

   注: この CSR は Apache 形式の証明書として識別されます。

内部の認証局によって署名された証明書

商用の証明書プロバイダーではなく、内部の認証局が証明書を発行した場合、証明書を正しく検証するには、内部のルート証明書がローカル証明書ストアに含まれるように QRadar を更新する必要があります。ルート検証証明書は、自動的にオペレーティング・システムに組み込まれます。

RedHat のトラスト・アンカー・ルート証明書ストアを更新するには、以下の手順を実行します。

1. CA のルート証明書を /etc/pki/ca-trust/source/anchors/ にコピーします。
2. SSH コマンド・ラインで以下のコマンドを実行します。

   ```
   update-ca-trust
   ```

QRadar コンソールへの新規 SSL 証明書のインストール

始める前に

以下のものが必要です。

- 内部 CA またはパブリック CA が発行した新規の署名証明書。
- CSR ファイルを生成するための qradar.key 秘密鍵。
- 中間証明書 (証明書プロバイダーが使用する場合)。

  注: 中間証明書を使用する場合、新しい証明書と中間証明書の両方をインストールするには、-i フラグを指定して「install-ssl-cert.sh」コマンドを実行します。中間証明書を使用する場合は、以下の 3 つのファイル・パスを入力するように求められます。

  – SSLCertificateFile
  – SSLIntermediateCertificateFile

– SSLCertificateKeyFile

手順

1. SSH を使用して QRadar コンソールに root ユーザーとしてログインします。
2. 以下のコマンドを入力して、証明書をインストールします。

```
[root@qavm215 ~]# /opt/qradar/bin/install-ssl-cert.sh
Path to Public Key File (SSLCertificateFile): /root/new.certs/cert.cert
Path to Private Key File (SSLCertificateKeyFile): /root/new.certs/cert.key
```

出力例:

```
You have specified the following:

       SSLCertificateFile of /root/updated.certs/cert.cert
    SSLCertificateKeyFile of /root/updated.certs/cert.key

Re-configure Apache now (includes restart of httpd) (Y/[N])? y
Backing up current SSL configuration ... (OK)
Installing user SSL certificate ... (OK)
Reloading httpd configuration:
 - Restarting httpd service ... (OK)
Restarting services:
 - Stopping hostcontext ... (OK)
 - Restarting Tomcat ... (OK)
 - Starting hostcontext ... (OK)
Tue Sep 19 14:45:57 ADT 2017 [install-ssl-cert.sh] OK: Install SSL Cert
   Completed
[root@qavm215 ~]#
```

3. 「管理」タブで、「拡張」 > 「すべての構成のデプロイ」をクリックします。

注: すべての構成をデプロイすると、QRadar によりすべてのサービスが再始動されます。イベントおよびフローに関するデータ収集は、デプロイが完了するまで停止します。

トラブルシューティング

証明書に関して問題がある場合 (名前または IP アドレスが正しくないなど)、有効期限が過ぎた場合、またはコンソールで IP またはホスト名を変更した場合、自己署名証明書に戻すことを選択できます。

自己署名証明書を生成するには、QRadar コンソールで以下の手順を実行します。

1. 以前インストールしたが、機能していない証明書をバックアップします。証明書の生成を実行すると、既存の証明書が検出され、報告されます。これにより、生成プロセスは停止します。

```
mkdir /root/backup.certs/
mv /etc/httpd/conf/certs/cert.* /root/backup.certs/
```

2. **/opt/qradar/bin/install-ssl-cert.sh –generate** コマンドを実行し、新しい証明書を生成します。このプロセスは、QRadar のインストール時に最初の SSL 証明書を生成するためにも使用されます。

```
[root@qavm215 certs]# /opt/qradar/bin/install-ssl-cert.sh --generate
Generating self-signed SSL certificate ... (OK)
Installing generated SSL certificate ... (OK)
Tue Sep 19 14:00:42 ADT 2017 [install-ssl-cert.sh] OK:
Generated SSL certificate installed successfully
[root@qavm215 certs]#
```

3. 新しく生成した証明書を新しいディレクトリーに移動します。
   install-ssl-cert.sh スクリプトをインストール・モードで使用して、新しい SSL 証明書をインストールおよび配布します。

```
[root@qavm215 ~]# mkdir /root/updated.certs/
[root@qavm215 ~]# mv /etc/httpd/conf/certs/cert.* /root/updated.certs/
[root@qavm215 ~]# /opt/qradar/bin/install-ssl-cert.sh
Path to Public Key File (SSLCertificateFile): /root/updated.certs/cert.cert
Path to Private Key File (SSLCertificateKeyFile): /root/updated.certs/cert.key

You have specified the following:

       SSLCertificateFile of /root/updated.certs/cert.cert
    SSLCertificateKeyFile of /root/updated.certs/cert.key

Re-configure Apache now (includes restart of httpd) (Y/[N])? y
Backing up current SSL configuration ... (OK)
Installing user SSL certificate ... (OK)
Reloading httpd configuration:
 - Restarting httpd service ... (OK)
Restarting services:
 - Stopping hostcontext ... (OK)
 - Restarting Tomcat ... (OK)
 - Starting hostcontext ... (OK)
Tue Sep 19 14:45:57 ADT 2017 [install-ssl-cert.sh] OK:
Install SSL Cert Completed
[root@qavm215 ~]#
```

QRadar デプロイメントでの IPv6 アドレス指定

IBM Security QRadar ソフトウェアおよびアプライアンスのネットワーク接続と管理のために、IPv4 と IPv6 のアドレス指定がサポートされています。QRadar のインストール時に、使用するインターネット・プロトコルが IPv4 であるか、IPv6 であるかを指定するよう求めるプロンプトが表示されます。

IPv6 アドレス指定に関する以下の詳細情報を確認してください。

『IPv6 アドレス指定をサポートする QRadar コンポーネント』

115 ページの『IPv6 環境または混合環境での QRadar のデプロイ』

116 ページの『IPv6 アドレス指定の制限』

IPv6 アドレス指定をサポートする QRadar コンポーネント

以下の QRadar のコンポーネントは、IPv6 のアドレス指定をサポートします。

「ネットワーク・アクティビティー」タブ

「**IPv6** 送信元アドレス **(IPv6 Source Address)**」および「**IPv6** 宛先アドレス **(IPv6 Destination Address)**」はデフォルトの列ではないため、自動的には表示されません。これらの列を表示するには、検索パラメーター (列定義) の構成時にこれらの列を選択する必要があります。

IPv4 または IPv6 の送信元環境でスペースを節約し、索引付けの作業を省くために、追加 IP アドレス・フィールドは保存されず、表示もされません。IPv4 と IPv6 が混在する環境では、フロー・レコードに IPv4 アドレスと IPv6 アドレスの両方が含まれます。

sFlow を含むパケット・データと NetFlow V9 データの両方で IPv6 アドレスがサポートされます。ただし、それより古いバージョンの NetFlow では、IPv6 がサポートされない場合があります。

「ログ・アクティビティー」タブ

「**IPv6** 送信元アドレス **(IPv6 Source Address)**」および「**IPv6** 宛先アドレス **(IPv6 Destination Address)**」はデフォルトの列ではないため、自動的には表示されません。これらの列を表示するには、検索パラメーター (列定義) の構成時にこれらの列を選択する必要があります。

DSM は、イベント・ペイロードから IPv6 アドレスを解析することができます。DSM で IPv6 アドレスを解析できない場合は、ログ・ソース拡張によりアドレスを解析することができます。ログ・ソース拡張について詳しくは、「*IBM Security QRadar Log Sources User Guide*」を参照してください。

IPv6 フィールドでの検索、グループ化、およびレポート作成

検索条件で IPv6 パラメーターを使用することにより、イベントとフローを検索することができます。

IPv6 パラメーターに基づいてイベント・レコードやフロー・レコードをグループ化したりソートしたりすることもできます。

IPv6 ベースの検索からのデータに基づいたレポートを作成することができます。

カスタム・ルール

IPv6 のアドレス指定をサポートするために、次のカスタム・ルールが追加されました: **SRC/DST IP = IPv6 Address**

IPv6 ベースのビルディング・ブロックを、他のルールで使用することができます。

デバイス・サポート・モジュール **(DSM)**

DSM は、IPv6 送信元アドレスと宛先アドレスをイベント・ペイロードから解析することができます。

IPv6 環境または混合環境での QRadar のデプロイ

IPv6 環境または混合環境の QRadar にログインするには、IP アドレスを以下のように大括弧で囲みます。

```
https://[<IP Address>]
```

IPv4 環境と IPv6 環境のどちらも、ホスト・ファイルを使用して、アドレス変換を行うことができます。IPv6 環境または混合環境では、クライアントはコンソール・アドレスをホスト名で解決します。IPv6 コンソールの IP アドレスを、クライアント上の `/etc/hosts` ファイルに追加する必要があります。

NetFlow や sFlow などのフロー・ソースは、IPv4 アドレスおよび IPv6 アドレスから受け入れられます。syslog や SNMP などのイベント・ソースは、IPv4 アドレスおよび IPv6 アドレスから受け入れられます。IPv6 環境では、スーパーフローとフロー・バンドルを無効にすることができます。

制約事項:
デフォルトでは、IPv6 と IPv4 の混合モードのコンソールに IPv4 のみの管理対象ホストを追加することはできません。IPv4 のみの管理対象ホストを有効にするスクリプトを実行する必要があります。

IPv6 アドレス指定の制限

IPv6 環境に QRadar をデプロイするときには、以下の制限があることがわかっています。

- ネットワーク階層は、IPv6 をサポートするように更新されません。

  監視、検索、分析を含む QRadar のデプロイメントのある部分では、ネットワーク階層が利用されません。例えば、「ログ・アクティビティー」タブ内では、イベントをネットワーク別に検索したり集約したりできません。
- IPv6 ベースのアセット・プロファイルはありません。
- QRadar が IPv4 ホストに関するイベント、フロー、脆弱性データを受信したときにのみ、アセット・プロファイルが作成されます。
- IPv6 アドレス用のカスタム・ルールには、ホスト・プロファイル・テストがありません。
- IPv6 アドレスの特殊な索引付けや最適化はありません。
- オフェンスには IPv6 ベースの送信元および宛先はありません。

混合環境での IPv4 のみの管理対象ホストのインストール

デフォルトでは、IBM Security QRadar 製品で、IPv6 と IPv4 の混合モードのコンソールに IPv4 のみの管理対象ホストを追加することはできません。IPv4 のみの管理対象ホストを有効にするスクリプトを実行する必要があります。

手順

1. IBM Security QRadar コンソールを、IPv6 のアドレス指定を選択してインストールします。
2. インストール後に、QRadar コンソールで次のコマンドを入力します。

   ```
   /opt/qradar/bin/setup_v6v4_console.sh
   ```
3. IPv4 管理対象ホストを追加するには、以下のコマンドを入力します。

   ```
   /opt/qradar/bin/add_v6v4_host.sh
   ```
4. 管理対象ホストを追加します。

関連タスク:

75 ページの『管理対象ホストの追加』
イベントおよびフロー・コレクター、イベントおよびフロー・プロセッサー、データ・ノードなどの管理対象ホストを追加して、データ収集およびデータ処理のアクティビティーを IBM Security QRadar デプロイメント全体に分散させます。

高度な iptables ルールの例

QRadar へのアクセスをより適切に制御したり、インバウンド・データ・ソースを制限したり、トラフィックをリダイレクトしたりするように iptables ルールを構成できます。以下の例では、iptables を手動で調整することで、ご使用のネットワークに対するより深い洞察を得られます。

SSH への iptables アクセスのブロック

コンソールおよび非管理対象ホストは、すべてのインバウンド要求の SSH を許可します。デプロイメントにホストを追加すると、コンソールは QRadar コンソールからの SSH アクセスを許可し、インバウンド接続に対してポート 22 を開いたままにします。ポート 22 のインバウンド接続を制限するには、ホストの iptables ルールを変更します。

暗号化された接続を切断する可能性のある他の管理対象ホストからの SSH アクセスをコンソールでブロックできます。

```
-A INPUT -i eth0 -m state --state NEW -m tcp -p tcp --dport 22 -s 10.100.50.41 -j ACCEPT
-A INPUT -i eth0 -m state --state NEW -m tcp -p tcp --dport 22 -s 10.100.50.59 -j ACCEPT
-A INPUT -i eth0 -m state --state NEW -m tcp -p tcp --dport 22 -j DROP
```

QRadar システムに対する ICMP の有効化

以下のルールを /opt/qradar/conf/iptables.pre ファイルに追加することで、QRadar システムからの ping 応答を有効にできます。

```
-A INPUT -p icmp -j ACCEPT
```

以下のスクリプトを実行して、/etc/sysconfig/iptables ファイル内にエントリーを作成します。

重要: このルールを特定のホストに限定するには、-s source.ip.address フィールドを追加します。

不要なデータ・ソースのブロック

ログ・ソースまたは netflow データ・ソースなどのデータ・ソースを、元のデバイスを無効にするのではなく、短時間ブロックできます。特定のホストをブロックするには、以下のようなエントリーを /opt/qradar/conf/iptables.pre に追加します。

ルーターからの netflow をブロックする場合:

```
-A INPUT -p udp -s <IP Address> --dport 2055 -j REJECT
```

別のソースからの Syslog をブロックする場合:

```
-A INPUT -p tcp -s <IP Address> --dport 514 -j REJECT
```

```
-A INPUT -p udp -s <IP Address> --dport 514 -j REJECT
```

特定のサブネットからの Syslog をブロックする場合:

```
-A INPUT -p tcp -s <IP Address> --dport 514 -j REJECT
```

```
-A INPUT -p udp -s <IP Address> --dport 514 -j REJECT
```

Syslog ポートへの iptables のリダイレクト

非標準ポートでの Syslog トラフィックを QRadar イベント・コレクターのポート 514 にリダイレクトできます。以下の手順を使用することで、iptables ルールで代替ポートを イベント・コレクターの 514 にリダイレクトできるようになります。

1. /etc/sysctl.conf ファイルで以下の行を追加するか、または更新して、Linux カーネルの NAT オプションを有効にします。

   ```
   net.ipv4.ip_forward = 1
   ```

   注: NAT ルールへの変更内容を有効にするには、サービスの再始動が必要になる場合があります。

2. 現在のアクティブなカーネルで IP フォワードを有効にします。

   ```
   echo 1 > /proc/sys/net/ipv4/ip_forward
   ```

3. 以下の行を /opt/qradar/conf/iptables-nat.post に追加します。リダイレクトするポート番号を *<portnumber>* として入力します。

   ```
   -A PREROUTING -p udp --dport <portnumber> -j REDIRECT --to-ports 514
   -A PREROUTING -p tcp --dport <portnumber> -j REDIRECT --to-ports 514
   ```

4. 以下のコマンドを入力して iptables を再作成します。

   ```
   /opt/qradar/bin/iptables_update.pl
   ```

5. 以下のコマンドを入力してリダイレクトを検証します。

   ```
   iptables -nvL -t nat
   ```

   以下のコードは出力の表示例です。 Chain PREROUTING (policy ACCEPT 140 packets, 8794 bytes) pkts bytes target prot opt in out source destination 0 0 REDIRECT udp -- * * 0.0.0.0/0 0.0.0.0/0 udp dpt:10529 redir ports 514 0 0 REDIRECT tcp -- * * 0.0.0.0/0 0.0.0.0/0 tcp dpt:10529 redir ports 514 Chain POSTROUTING (policy ACCEPT 207 packets, 25772 bytes) pkts bytes target prot opt in out source destination Chain OUTPUT (policy ACCEPT 207 packets, 25772 bytes) pkts bytes target prot opt in out source destination

インバウンド Syslog トラフィックのリダイレクト

QRadar コンソール を Syslog メッセージ・ゲートウェイとして使用し、iptables のルールを構成してインバウンド・イベントをリダイレクトできます。

1. イベント・コレクターでログ・ソースの転送ルールを有効にします。
2. TCP Syslog の宛先転送をポート 7780 のコンソール IP アドレスに設定します。
3. コンソールのコマンド・ラインで、別のホストにリダイレクトするための以下の iptables ルールを追加します。

   ```
    iptables -I OUTPUT --src 0/0 --dst 153.2.200.80 -p
   tcp --dport 7780 -j REDIRECT --to-ports 514
   ```

iptables ルールの構成

QRadar ネットワーク・サービスへのアクセスは、最初にホスト上で iptables を使用して制御されます。iptables ルールは、デプロイメント環境の要件に基づいて調

整および構成されます。Ariel 検索、ストリーミング、および暗号化 (トンネリング) の使用時の各ポートは、各種 iptables ルールを更新できます。

このタスクについて

IPv4 および IPv6 に対する iptables ルールを構成および確認できます。以下の手順は、iptables を手動で調整する方法を示しています。

手順

1. SSH を使用して、root ユーザーとして QRadar にログインします。

   ログイン: <root>

   パスワード: <password>
2. 以下のコマンドを入力して、プレ・ルール iptables ファイルを編集します。

   IPv4:

   ```
   vi /opt/qradar/conf/iptables.pre
   ```

   IPv6:

   ```
   vi /opt/qradar/conf/ip6tables.pre
   ```

   iptables.pre 構成ファイルが表示されます。
3. 以下のコマンドを入力して、ポスト・ルール iptables ファイルを編集します。

   IPv4:

   ```
   vi /opt/qradar/conf/iptables.post
   ```

   IPv6:

   ```
   vi /opt/qradar/conf/ip6tables.post
   ```

   iptables.post 構成ファイルが表示されます。
4. 特定のポート番号にアクセスするための QRadar の以下のルールを追加します。ここで、*portnumber* はそのポート番号です。

   特定のポート入力の UDP トラフィックを受け入れる場合:

   ```
   -A INPUT -m udp -p udp --dport <portnumber> -j ACCEPT
   ```

   特定のポート入力の TCP トラフィックを受け入れる場合:

   ```
   -A INPUT -m state --state NEW -m tcp -p tcp --dport <portnumber> -j
   ACCEPT
   ```
5. iptables 構成を保存します。
6. 以下のスクリプトを実行して、変更内容を伝搬させます。

   ```
   /opt/qradar/bin/iptables_update.pl
   ```
7. 以下のコマンドを入力して、既存の iptables を確認します。

IPv4:

```
iptables -L -n -v
```

IPv6:

```
ip6tables -L -n -v
```

データ保存

保存バケットは、イベント・データおよびフロー・データを IBM Security QRadar で保持する期間を定義します。

QRadar がイベントおよびフローを受信すると、各イベントおよびフローが保存バケットのフィルター基準と比較されます。イベントまたはフローが保存バケットのフィルターと一致した場合、そのイベントまたはフローは、削除ポリシーの期間に到達するまでその保存バケットに保管されます。

保存バケットは、上の行から下の行に優先順位に従って配列されます。レコードは、優先順位が最も高いフィルター基準と一致するバケットに保管されます。レコードが、構成済みの保存バケットのいずれとも一致しない場合、そのレコードはデフォルトの保存バケット (構成可能な保存バケットのリストの下に常に置かれる) に保管されます。

テナント・データ

共有データに対して最大 10 個の保存バケットを構成でき、各テナントに対して最大 10 個の保存バケットを構成できます。

データがシステムに到達すると、データが評価され、それが共有データかテナントに属するデータかが判別されます。テナント固有のデータは、そのテナントに対して定義されている保存バケット・フィルターと比較されます。データが保存バケットのフィルターと一致すると、そのデータは保存ポリシーの期間に到達するまで保存バケットに格納されます。

テナントに対して保存バケットを構成していない場合、データは自動的にそのテナントのデフォルト保存バケットに配置されます。

保存バケットの構成

保存ポリシーを構成して、IBM Security QRadar がイベント・データとフロー・データを保持する必要がある期間と、そのデータが特定の存続期間に達したときの処理を定義します。

このタスクについて

保存バケット・フィルターに対する変更は、受信データのみに即時に適用されます。例えば、ソース IP アドレス 10.0.0.0/8 からのすべてのデータを 1 日間保持する保存バケットを構成し、後でフィルターを編集してソース IP 192.168.0.1 からのデータを保持するようにした場合、その変更が遡及的に適用されることはありませ

ん。フィルターを変更すると即時に、保存バケットには 10.0.0.0/8 の 24 時間のデータが保持され、フィルターの変更後に収集されるデータはすべて 192.168.0.1 のデータになります。

バケットに対する保存ポリシーは、フィルター基準に関係なくバケット内のすべてのデータに適用されます。前述の例を使用して保存ポリシーを 1 日間から 7 日間に変更した場合、バケット内の 10.0.0.0/8 データと 192.168.0.1 データの両方が 7 日間保持されます。

保存バケットの「分布」は、保存バケットの使用量を、すべての保存バケット内のデータ保存の合計のパーセンテージとして示します。分布は、テナントごとのベースで計算されます。

手順

1. 「管理」タブをクリックします。
2. ナビゲーション・メニューで、「データ・ソース」をクリックします。
3. 「イベント保存」または「フロー保存」アイコンをクリックします。
4. テナントを構成済みの場合は、「テナント」リストで、保存バケットの適用先とするテナントを選択します。

   注**:** マルチテナント構成で共有データの保存ポリシーを管理するには、「テナント」リストで「**N/A**」を選択してください。
5. 新規の保存バケットを構成するには、以下の手順を実行します。
   a. テーブルの最初の空の行をダブルクリックして「保存プロパティー」ウィンドウを開きます。
   b. 保存バケット・パラメーターを構成します。

      保存バケット・パラメーターに関する詳細の説明**:**

プロパティー	説明
名前	保存バケットの固有名を入力します。
データをこのバケットに保持する期間	データが保持される期間を指定する保存期間。保存期間が経過すると、データが「**このバケット内のデータの削除 (Delete data in this bucket)**」パラメーターに従って削除されます。QRadar は、保存期間内のデータを削除することはありません。

プロパティー	説明
このバケットのデータを削除	**「データをこのバケットに保持する期間」**パラメーターと一致した時点で直ちにデータを削除する場合は、「保存期間が満了した直後」を選択します。データは、ディスク・ストレージ要件とは関係なく、次のスケジュール済みディスク保守プロセス時に削除されます。 ディスク・モニター・システムによってストレージが必要であることが検出されるまで、**「データをこのバケットに保持する期間」**パラメーターと一致するデータをストレージに保持しておく場合は、「ストレージ・スペースが必要な場合」を選択します。 ストレージ・スペースに基づく削除は、空きディスク・スペースが 15% 以下に低下したときに開始され、空きディスク・スペースが 18% になるか、「データをこのバケットに保持する期間」フィールドに設定されたポリシーの時間フレームが経過するまで削除が続行されます。例えば、レコードの使用ディスク・スペースが 85% に達した場合、使用パーセンテージが 82% に低下するまでデータが削除されます。ストレージが必要な場合は、「データをこのバケットに保持する期間」フィールドと一致するデータのみが削除されます。 バケットが「このバケットのデータを削除**:** 保存期間が満了した直後」に設定されている場合は、ディスク・スペースの検査は一切実行されず、保存期間を経過したすべてのデータが削除タスクによって直ちに削除されます。
説明	保存バケットの説明を入力します。
現在のフィルター **(Current Filters)**	各データが比較されるフィルター基準を構成します。

c. フィルター基準の各セットの指定後に「フィルターの追加」をクリックします。

d. 「保存」をクリックします。

6. 既存の保存バケットを編集するには、テーブルから行を選択し、「編集」をクリックします。

   保存ポリシー・プロパティーについては、ステップ 5 を参照してください。

7. 保存バケットを削除するには、テーブルから行を選択し、「削除」をクリックします。

8. 「保存」をクリックします。

   保存ポリシー・プロパティーと一致する受信データが直ちに保存バケットに保管されます。

保存バケット順序の管理

保存バケットの順序を変更して、データが、要件と一致する順序で保存バケットと突き合わされるようにすることができます。

このタスクについて

保存バケットは、「イベント保存」ウィンドウと「フロー保存」ウィンドウで、上の行から下の行に優先順位に従って配列されます。レコードは、レコード・パラメーターと一致する最初の保存バケットに保管されます。

デフォルトの保存バケットを移動することはできません。これは、常にリストの下部にあります。

手順

1. 「管理」タブをクリックします。
2. ナビゲーション・メニューで、「データ・ソース」をクリックします。
3. 「イベント保存」または「フロー保存」アイコンをクリックします。
4. テナントを構成済みの場合は、「テナント」リストで、保存バケットを再配列するテナントを選択します。

   注: マルチテナント構成で共有データの保存ポリシーを管理するには、「テナント」リストで「**N/A**」を選択してください。
5. 移動対象の保存バケットに対応する行を選択し、「上へ」または「下へ」をクリックして、適切な場所に移動します。
6. 「保存」をクリックします。

保存バケットの有効化および無効化

保存バケットを構成して保存すると、デフォルトで有効になります。イベント保存またはフロー保存をチューニングするために、バケットを無効にすることができます。

このタスクについて

バケットを無効にすると、無効になっているバケットの要件と一致する新規のイベントまたはフローは、イベント・プロパティーまたはフロー・プロパティーと一致する次のバケットに保管されます。

手順

1. 「管理」タブをクリックします。
2. ナビゲーション・メニューで、「データ・ソース」をクリックします。
3. 「イベント保存」または「フロー保存」アイコンをクリックします。
4. テナントを構成済みの場合は、「テナント」リストで、保存バケットを変更するテナントを選択します。

   注: マルチテナント構成で共有データの保存ポリシーを管理するには、「テナント」リストで「**N/A**」を選択してください。
5. 無効にする保存バケットを選択して、「有効/無効」をクリックします。

保存バケットの削除

保存バケットを削除すると、その保存バケットに含まれているイベントまたはフローはシステムから削除されず、そのバケットを定義している基準のみが削除されます。すべてのイベントまたはフローはストレージ内に維持されます。

このタスクについて

保存バケットを削除すると、その保存バケットに含まれているデータはシステムから削除されず、そのバケットを定義している基準のみが削除されます。すべてのデータはストレージ内に維持されます。

手順

1. 「管理」タブをクリックします。
2. ナビゲーション・メニューで、「データ・ソース」をクリックします。
3. 「イベント保存」アイコンまたは「フロー保存」アイコンをクリックします。
4. テナントを構成済みの場合は、「テナント」リストで、保存バケットを削除するテナントを選択します。

   注**:** マルチテナント構成で共有データの保存ポリシーを管理するには、「テナント」リストで「**N/A**」を選択してください。
5. 削除する保存バケットを選択して、「削除」をクリックします。

システム通知の構成

しきい値のシステム・パフォーマンス・アラートを構成できます。このセクションでは、システムのしきい値の構成について説明します。

このタスクについて

以下の表で、「グローバル・システム通知 (Global System Notifications)」ウィンドウのパラメーターについて説明します。

表 *20.* 「グローバル・システム通知 *(Global System Notifications)*」ウィンドウのパラメーター

パラメーター	説明
過去 1 分間のシステム負荷 (System load over 1 minute)	過去 1 分間の平均システム負荷のしきい値を入力します。
過去 5 分間のシステム負荷 (System load over 5 minutes)	過去 5 分間の平均システム負荷のしきい値を入力します。
過去 15 分間のシステム負荷 (System load over 15 minutes)	過去 15 分間の平均システム負荷のしきい値を入力します。
デバイスの入出力要求の平均時間 (ミリ秒)	入出力要求のしきい値時間 (ミリ秒) を入力します。
使用スワップのパーセンテージ (Percentage of swap used)	使用スワップ・スペースのパーセンテージのしきい値を入力します。
1 秒当たりの受信パケット数 (Received packets per second)	1 秒当たりに受信されるパケット数のしきい値を入力します。

表 20. 「グローバル・システム通知 *(Global System Notifications)*」ウィンドウのパラメーター *(続き)*

パラメーター	説明
1 秒当たりの送信パケット数 (Transmitted packets per second)	1 秒当たりに送信されるパケット数のしきい値を入力します。
1 秒当たりの受信バイト数 (Received bytes per second)	1 秒当たりに受信されるバイト数のしきい値を入力します。
1 秒当たりの送信バイト数 (Transmitted bytes per second)	1 秒当たりに送信されるバイト数のしきい値を入力します。
受信エラー数 (Receive errors)	1 秒当たりに受信される破損パケット数のしきい値を入力します。
送信エラー数 (Transmit errors)	1 秒当たりに送信される破損パケット数のしきい値を入力します。
パケット衝突数 (Packet collisions)	パケットの送信中に 1 秒当たりに発生する衝突数のしきい値を入力します。
ドロップされる受信パケット数 (Dropped receive packets)	バッファー内のスペース不足のためにドロップされる 1 秒当たりの受信パケット数のしきい値を入力します。
ドロップされる送信パッケージ数 (Dropped transmit packets)	バッファー内のスペース不足のためにドロップされる 1 秒当たりの送信パケット数のしきい値を入力します。
送信キャリア・エラー数 (Transmit carrier errors)	パケットの送信中に 1 秒当たりに発生するキャリア・エラー数のしきい値を入力します。
受信フレーム・エラー数 (Receive frame errors)	受信パケットで 1 秒当たりに発生するフレーム・アライメント・エラー数のしきい値を入力します。
受信 FIFO オーバーラン数 (Receive fifo overruns)	受信パケットで 1 秒当たりに発生する先入れ先出し法 (FIFO) オーバーラン・エラー数のしきい値を入力します。
送信 FIFO オーバーラン数 (Transmit fifo overruns)	送信パケットで 1 秒当たりに発生する先入れ先出し法 (FIFO) オーバーラン・エラー数のしきい値を入力します。

手順

1. 「管理」タブをクリックします。
2. ナビゲーション・メニューで、「システム構成」をクリックします。
3. 「グローバル・システム通知 **(Global System Notifications)**」アイコンをクリックします。
4. 構成するパラメーターごとに、値を入力します。
5. 各パラメーターで、「有効」および「応答基準」を選択し、次のオプションのいずれかを選択します。

オプション	説明
「次より大」	パラメーター値が構成されている値を超えるとアラートが発生します。

オプション	説明
「次より小」	パラメーター値が構成されている値より小さいとアラートが発生します。

6. アラートに対して推奨される解決策の説明を入力します。
7. 「保存」をクリックします。
8. タブ・メニューで、「変更のデプロイ」をクリックします。

カスタムの E メール通知の構成

IBM Security QRadar でルールを構成するときには、ルールの応答が生成されるたびに、受信者に E メール通知を送信するように指定します。この E メール通知は、イベントやフローのプロパティーなどの有用な情報を提供します。

このタスクについて

alert-config.xml ファイルを編集することによって、E メール通知にルールの応答として組み込まれる内容をカスタマイズすることができます。

注: IBM QRadar Log Manager には、フローに対する参照は適用されません。

一時ディレクトリーを作成しておき、このディレクトリーで、デフォルト・ファイルを上書きしてしまう恐れなしに、安全にファイルのコピーを編集できるようにする必要があります。alert-config.xml ファイルを編集し保存した後、行った変更を検証するスクリプトを実行する必要があります。検証スクリプトにより変更内容が自動的にステージング・エリアに適用され、その後変更内容を実稼働環境にデプロイできます。

手順

1. SSH を使用して、root ユーザーとして QRadar コンソールにログインします。
2. デフォルト・ファイルのコピーを安全に編集するために使用する、一時ディレクトリーを新規作成します。
3. custom_alerts ディレクトリーに格納されているファイルを、作成した一時ディレクトリーにコピーするために、次のコマンドを入力します。

   ```
   cp /store/configservices/staging/globalconfig/templates/
   custom_alerts/*.* <directory_name>
   ```

   <*directory_name*> オプションは、作成した一時ディレクトリーの名前です。
4. ファイルが正常にコピーされたことを、次のようにして確認します。
   a. ディレクトリーにあるファイルをリストするために、次のコマンドを入力します。

      ```
      ls -lah
      ```

   b. 次のファイルがリストされていることを確認します。

      ```
      alert-config.xml
      ```

5. 編集のために alert-config.xml ファイルを開きます。

6. 複数のテンプレート・エレメントを作成するには、以下の <template></template> エレメント (タグと内容を含む) をコピーして、既存の <template></template> エレメントの下に貼り付けます。

```
<template>
  <templatename>Default Flow</templatename>
  <templatetype>flow</templatetype>
  <active>true</active>
  <filename></filename>
  <subject>${RuleName} Fired </subject>
  <body>
     The ${AppName} event custom rule engine sent an automated response:

     ${StartTime}

     Rule Name:                                      ${RuleName}
     Rule Description:                               ${RuleDescription}

     Source IP:                                      ${SourceIP}
     Source Port:                                    ${SourcePort}
     Source Username (from event):                   ${UserName}
     Source Network:                                 ${SourceNetwork}

     Destination IP:                                 ${DestinationIP}
     Destination Port:                               ${DestinationPort}
     Destination Username (from Asset Identity):     ${DestinationUserName}
     Destination Network:                            ${DestinationNetwork}

     Protocol:                                       ${Protocol}
     QID:                                            ${Qid}

     Event Name:                                     ${EventName}
     Event Description:                              ${EventDescription}
     Category:                                       ${Category}

     Log Source ID:                                  ${LogSourceId}
     Log Source Name:                                ${LogSourceName}

     Payload:                                        ${Payload}

     CustomPropertiesList:                           ${CustomPropertiesList}

   </body>
   <from></from>
   <to></to>
   <cc></cc>
   <bcc></bcc>
</template>
```

重要: QRadar でオプションとして表示させるイベント・テンプレート・タイプおよびフロー・テンプレート・タイプごとに、<active></active> プロパティーを True に設定する必要があります。<filename></filename> プロパティーを空のままにしておく必要もあります。

7. <template></template> エレメントの内容を編集します。
   a. 次の XML プロパティーを使用して、テンプレート・タイプを指定します。

      ```
      <templatetype></templatetype>
      ```

      指定可能な値は、event または flow です。この値は必須です。
   b. 次の XML エレメントを使用して、テンプレート名を指定します。

```
<templatename></templatename>
```

c. 次のようにして、アクティブ・エレメントを true に設定します。

```
<active>true</active>
```

d. 必要に応じて、subject エレメントを編集します。

e. 必要に応じて、body エレメントまたは subject エレメントのパラメーターを追加または削除します。有効なパラメーターについては、指定可能なパラメーターの表を参照してください。

f. 追加するテンプレートごとに、これらのステップを繰り返します。

8. ファイルを保存して閉じます。

9. 行った変更を検証するために、次のコマンドを入力します。

```
/opt/qradar/bin/runCustAlertValidator.sh <directory_name>
```

<directory_name> オプションは、作成した一時ディレクトリーの名前です。

スクリプトによって変更が正常に検証されると、以下のメッセージが表示されます。

```
File alert-config.xml was deployed successfully to staging!
```

10. QRadar にログインします。

11. 「管理」タブをクリックします。

12. 「拡張」 > 「すべての構成のデプロイ」を選択します。

完全構成をデプロイすると、QRadar によりすべてのサービスが再始動されます。イベントおよびフローに関するデータ収集は、デプロイが完了するまで停止します。

例

表 *21.* 指定可能な通知パラメーター

共通パラメーター	イベント・パラメーター	フロー・パラメーター
AppName	EventCollectorID	Type
RuleName	DeviceId	CompoundAppID
RuleDescription	DeviceName	FlowSourceIDs
EventName	DeviceTime	SourceASNList
EventDescription	DstPostNATPort	DestinationASNList
EventProcessorId	SrcPostNATPort	InputIFIndexList
Qid	DstMACAddress	OutputIFIndexList
Category	DstPostNATIPAddress	AppId
RemoteDestinationIP	DstPreNATIPAddress	Host
Payload	SrcMACAddress	Port
Credibility	SrcPostNATIPAddress	SourceBytes
Relevance	SrcPreNATIPAddress	SourcePackets
Source	SrcPreNATPor	Direction
SourcePort	DstPreNATPort	SourceTOS
SourceIP		SourceDSCP

表 21. 指定可能な通知パラメーター (続き)

共通パラメーター	イベント・パラメーター	フロー・パラメーター
Destination		SourcePrecedence
DestinationPort		DestinationTOS
DestinationIP		DestinationDSCP
DestinationUserName		SourceASN
Protocol		DestinationASN
StartTime		InputIFIndex
Duration		OutputIFIndex
StopTime		FirstPacketTime
EventCount		LastPacketTime
SourceV6		TotalSourceBytes
DestinationV6		TotalDestinationBytes
UserName		TotalSourcePackets
DestinationNetwork		TotalDestinationPackets
SourceNetwork		SourceQOS
Severity		DestinationQOS
CustomPropertiesList		SourcePayload

カスタム・オフェンスのクローズ理由

「オフェンス」タブの「クローズの理由」リスト・ボックスにリストされるオプションを管理できます。

ユーザーが「オフェンス」タブでオフェンスをクローズすると、「オフェンスのクローズ」ウィンドウが表示されます。「クローズの理由」リスト・ボックスで理由を選択するためのプロンプトがユーザーに対して表示されます。以下の 3 つのデフォルトのオプションがリストされます。

- フォールス・ポジティブ、チューニング済み (False-positive, tuned)
- 問題なし (Non-issue)
- ポリシー違反 (Policy violation)

管理者は、「管理」タブでカスタム・オフェンスのクローズ理由を追加、編集、および削除できます。

カスタム・オフェンスのクローズ理由の追加

カスタム・オフェンスのクローズ理由を追加すると、新しい理由が、「カスタム・クローズ理由 (Custom Close Reasons)」ウィンドウと、「オフェンス」タブの「オフェンスのクローズ」ウィンドウの「クローズの理由」リスト・ボックスにリストされます。

このタスクについて

「カスタム・オフェンスのクローズ理由 (Custom Offense Close Reasons)」ウィンドウには、以下のパラメーターがあります。

表 22. 「カスタム・クローズ理由 *(Custom Close Reasons)*」ウィンドウのパラメーター

パラメーター	説明
理由 (Reason)	「オフェンス」タブの「オフェンスのクローズ」ウィンドウの「クローズの理由」リスト・ボックスに表示される理由。
作成者 (Created by)	このカスタム・オフェンスのクローズ理由を作成したユーザー。
作成日 (Date Created)	ユーザーがこのカスタム・オフェンスのクローズ理由を作成した日時。

手順

1. 「管理」タブをクリックします。
2. ナビゲーション・メニューで、「システム構成」をクリックします。
3. 「カスタム・オフェンスのクローズ理由」アイコンをクリックします。
4. 「追加」をクリックします。
5. オフェンスをクローズする固有の理由を入力します。理由は 5 文字から 60 文字の長さにする必要があります。
6. 「**OK**」をクリックします。 新しいカスタム・オフェンスのクローズ理由が、「カスタム・クローズ理由 (Custom Close Reason)」ウィンドウにリストされます。「オフェンス」タブの「オフェンスのクローズ」ウィンドウの「クローズの理由」リスト・ボックスにも、追加したカスタム理由が表示されます。

カスタム・オフェンスのクローズ理由の編集

カスタム・オフェンスのクローズ理由を編集すると、「カスタム・クローズ理由 (Custom Close Reasons)」ウィンドウ内と、「オフェンス」タブの「オフェンスのクローズ」ウィンドウの「クローズの理由」リスト・ボックス内で、その理由が更新されます。

手順

1. 「管理」タブをクリックします。
2. ナビゲーション・メニューで、「システム構成」をクリックします。
3. 「カスタム・オフェンスのクローズ理由」アイコンをクリックします。
4. 編集する理由を選択します。
5. 「編集」をクリックします。
6. オフェンスをクローズする新しい固有の理由を入力します。理由は 5 文字から 60 文字の長さにする必要があります。
7. 「**OK**」をクリックします。

カスタム・オフェンスのクローズ理由の削除

カスタム・オフェンスのクローズ理由を削除すると、「カスタム・クローズ理由 (Custom Close Reasons)」ウィンドウと、「オフェンス」タブの「オフェンスのクローズ」ウィンドウの「クローズの理由」リスト・ボックスから、その理由が削除されます。

手順

1. 「管理」タブをクリックします。
2. ナビゲーション・メニューで、「システム構成」をクリックします。
3. 「カスタム・オフェンスのクローズ理由」アイコンをクリックします。
4. 削除する理由を選択します。
5. 「削除」をクリックします。
6. 「**OK**」をクリックします。

カスタム・アセット・プロパティーの構成

アセット・プロパティーを定義して、アセット照会を容易にします。カスタム・プロパティーには、より多くの照会オプションがあります。

手順

1. 「管理」タブをクリックします。
2. 「カスタム・アセット・プロパティー」をクリックします。
3. 「名前」フィールドに、カスタム・アセット・プロパティーの記述子を入力します。
4. 「タイプ」ドロップダウン・メニューで、「数値」または「テキスト」を選択して、カスタム・アセット・プロパティーの情報タイプを定義します。
5. 「**OK**」をクリックします。
6. 「アセット」タブをクリックします。
7. 「アセットの編集」 > 「カスタム・アセット・プロパティー」をクリックします。
8. 値フィールドに必要な情報を入力してください。
9. 「**OK**」をクリックします。

索引管理

索引管理を使用して、イベント・プロパティーとフロー・プロパティーのデータベース索引付けを制御します。IBM Security QRadar での検索速度を上げるために、検索照会に索引付きフィールドを追加してデータ全体の絞り込みを行います。

索引 とは、ファイル内のデータおよびファイル・システム内のそのデータの位置に関する情報を指定する 1 組の項目のことです。データ索引は、データがストリーミングされているときにリアルタイムで作成されるか、データ収集後に要求に応じて作成されます。索引を使用するシステムでは、一致を検出するために各データをすべて読み通す必要がないため、検索効率が向上します。索引には、データ内の固有の用語とそれらの位置へのリファレンスが含まれています。索引によってディスク・スペースが使用されるため、検索時間を短縮するためにストレージ・スペースが使用される可能性があります。

検索を最適化するために、最初にイベント・プロパティーとフロー・プロパティーの索引付けを使用します。「索引管理 (Index Management)」ウィンドウにリストされているどのプロパティーに対しても索引付けを有効にすることができ、複数のプロパティーの索引付けも行うことができます。QRadar で検索を開始すると、検

索エンジンでは最初に、索引付けされたプロパティーによってデータ・セットがフィルタリングされます。索引付けされたフィルターを使用すると、データ・セットの一部が除外され、全体的なデータ量および検索対象のイベント・ログまたはフロー・ログの数が少なくなります。フィルターを使用しない場合、大規模なデータ・セットでは QRadar から結果が返されるまでの時間がより長くなります。

例えば、過去 6 カ月のログのうち**「この操作は許可されません」**という文章と一致するものをすべて検出するとします。デフォルトでは、QRadar には過去 30 日間のフルテキスト索引付けが保管されています。そのため、過去 6 カ月を対象に検索を行うには、システムはその時間フレーム内のすべてのイベントまたはフローのすべてのペイロード値を再読み取りして一致を見つけなければなりません。「ログ・ソース・タイプ」、「イベント名」、「送信元 **IP**」などの索引付き値フィルターを使用して検索すると、結果の表示速度が上がります。

「索引管理 (Index Management)」機能では、以下のような統計も提供されます。

- デプロイメントで実行されている保存済み検索 (索引付きプロパティーを含む) のパーセンテージ
- 選択した時間フレーム中に索引によってディスクに書き込まれるデータの量

ペイロード索引付けを有効にするには、「クイック・フィルター (Quick Filter)」プロパティーで索引付けを有効にする必要があります。

索引付けの有効化

「索引管理 (Index Management)」ウィンドウには、索引付け可能なすべてのイベント・プロパティーおよびフロー・プロパティーがリストされ、これらのプロパティーの統計が示されます。ツールバーのオプションにより、選択されたイベント・プロパティーおよびフロー・プロパティーの索引付けを、有効および無効にすることができます。

このタスクについて

データベース索引付けを変更すると、システム・パフォーマンスが低下する可能性があります。多数のプロパティーの索引付けを有効にした後は、統計をモニターするようにしてください。

手順

1. 「管理」タブをクリックします。
2. ナビゲーション・メニューで、「システム構成」をクリックします。
3. 「索引管理 **(Index Management)**」アイコンをクリックします。
4. 「索引管理 (Index Management)」リストから 1 つ以上のプロパティーを選択します。
5. 次のオプションのいずれかを選択してください。

状況	時間フレーム	アクション	理由 **(Reason)**
索引が無効であり、「プロパティーを使用している検索の **%**」が 30% を超え、「索引が欠落している検索の **%**」が 30% を超えている。	24 時間、7 日、または 30 日	「索引の有効化 **(Enable Index)**」をクリックします。	この検索プロパティーは頻繁に使用されています。索引を有効にするとパフォーマンスが向上する可能性があります。
索引が有効であり、「プロパティーを使用している検索の **%**」がゼロである。	30 日	「索引の無効化 **(Disable Index)**」をクリックします。	有効になっている索引が検索で使用されていません。索引付きのプロパティーを無効にして、ディスク・スペースを確保します。

6. 「保存」をクリックします。
7. 「**OK**」をクリックします。

タスクの結果

イベント・プロパティーおよびフロー・プロパティーが含まれているリストで、`[Indexed]` というテキストが、索引付けされたプロパティー名に付加されます。このようなリストの例として、「ログ・アクティビティー」タブおよび「ネットワーク・アクティビティー」タブの検索条件ページの検索パラメーターや、「フィルターの追加 (Add Filter)」ウィンドウの検索パラメーターなどがあります。

検索時間を最適化するためのペイロード索引の有効化

イベントおよびフローの検索時間を最適化するために、「クイック・フィルター」プロパティーでペイロード索引を有効にします。

制約事項**:**

「ログ・アクティビティー」タブおよび「ネットワーク・アクティビティー」タブの「クイック・フィルター」機能により、テキスト・ストリングを使用してイベントおよびフローのペイロードを検索することができます。ペイロード索引により、ディスク・ストレージ要件が増えるため、システム・パフォーマンスに影響を与える恐れがあります。デプロイメントが以下の条件を満たす場合に、ペイロード索引を有効にしてください。

- イベント・プロセッサーおよびフロー・プロセッサーのディスク使用率が 70% 未満である。
- イベント・プロセッサーおよびフロー・プロセッサーのレーティングが、1 秒当たりの最大イベント数 (EPS) またはインターフェース当たりの最大フロー数 (FPI) の 70% 未満である。

手順

1. IBM Security QRadar 製品の「管理」タブのナビゲーション・ペインで、「システム構成」をクリックします。

2. 「索引管理」をクリックします。
3. 「クイック検索」フィールドに「**クイック・フィルター**」と入力します。

   「クイック・フィルター」プロパティーが表示されます。
4. 索引付けする「クイック・フィルター」プロパティーを選択します。

   結果の表内の「データベース」列の値を使用して、フローまたはイベントの「クイック・フィルター」プロパティーを識別します。
5. ツールバーで、「索引の有効化」をクリックします。

   緑の点は、ペイロード索引が有効になっていることを示します。

   索引付けされたイベントまたはフローのプロパティーがリストに含まれている場合、プロパティー名の末尾に [Indexed] というテキストが付加されています。
6. 「保存」をクリックします。

次のタスク

ペイロード索引を管理するには、『ペイロード索引の保存期間の構成』を参照してください。

ペイロード索引の保存期間の構成

デフォルトの場合、IBM Security QRadar ではペイロード索引のデータ保存期間は 30 日に設定されます。QRadar でデフォルトの保存期間を変更すると、30 日を超えたクイック・フィルター索引の特定の値の検索が可能になります。

始める前に

完全なペイロード索引付けを有効にするには、ご使用の仮想アプライアンスおよび物理アプライアンスに最小で 24 GB の RAM が必要です。ただし、48 GB の RAM が推奨されています。

RAM の最小値と推奨値は、イベントまたはフローを処理するすべての QRadar システム (例えば、16xx、17xx、または 18xx のアプライアンス) に適用されます。

このタスクについて

保存の値は、検索にかかっている標準的な期間を反映しています。最短の保存期間は 1 日で、最長の保存期間は 2 年です。

手順

1. 「管理」タブをクリックします。
2. ナビゲーション・メニューで、「システム構成」をクリックします。
3. 「システム設定」をクリックします。
4. 「データベース設定」セクションで、「ペイロード索引の保存」リストから保存期間を選択します。
5. 「保存」をクリックします。
6. 「システム設定」ウィンドウを閉じます。
7. 「管理」タブ・メニューで、「変更のデプロイ」をクリックします。

次のタスク

デフォルト値より長い期間ペイロード索引を保存する場合は、追加のディスク・スペースが使用されます。「ペイロード索引の保存」フィールドで大きい値を選択した後は、システム通知をモニターして、ディスク・スペースが満杯になっていないか確認してください。

リソース負荷の高い検索を防止するための制限

IBM Security QRadar イベントおよびフローの検索に対してリソース制限を設定することにより、QRadar インフラストラクチャーの使用法のバランスを取ることができます。

リソース制限を設定する前に、ご使用の環境における通常の運用手順を慎重に検討してください。すべてのユーザーが自分が必要とするデータにアクセスできることが確保されている一方で、ユーザーがシステム可用性および他のユーザーのパフォーマンスに悪影響を及ぼす大規模な照会を不用意に実行するのを防止する制限を設定するようにしてください。

リソース制限のタイプ

ユーザー、ロール、またはテナントに基づいて時間制限またはデータ・セット制限を構成することにより、検索に対して制限を設定できます。

リソース制限は、ユーザー、ユーザー・ロール、テナントの順番で適用されます。例えば、ユーザーに対して設定されている制限は、そのユーザーが割り当てられているユーザー・ロールまたはテナントに対して設定されている制限よりも優先されます。

イベントおよびフローの検索に対して以下のタイプの制限を設定することができます。

- データを返すまでの検索の実行時間
- 検索対象データの時間幅
- Ariel 照会サーバーによって処理されるレコードの数。

ユーザー・ベースの制限

ユーザー・ベースの制限は、個々のユーザーの限度を定義します。この制限は、ロールおよびテナントの制限よりも優先されます。

例えば、SOC の下級アナリストとともに作業する大学生を組織が雇うとします。大学生には他の下級アナリストと同じユーザー・ロールを付与しますが、大学生が QRadar 照会のビルドに関して適切にトレーニングを受けるまではより厳格なユーザー・ベースの制限を適用します。

ロール・ベースの制限

ロール・ベースの制限を使用すると、QRadar デプロイメントへのさまざまなレベルのアクセス権限を必要とするユーザーのグループを定義できます。ロール・ベースの制限を設定することにより、さまざまなタイプのユーザーのニーズのバランスを取ることができます。

例えば、下級セキュリティー・アナリストは最近発生したセキュリティー・インシデントに焦点を当てる一方で、上級セキュリティー・アナリストはより長い期間にわたってデータのレビューを行うフォレンジック調査により関与する場合があります。ロール・ベースの制限を設定することにより、下級アナリストは過去 7 日間のデータのみにアクセスするように制限する一方で、上級アナリストはより長い時間幅のデータにアクセスできるようにすることが可能です。

テナント・ベースの制限

マネージド・セキュリティー・サービス・プロバイダー (MSSP) または複数の部門がある組織では、テナント・ベースの制限を使用すると、リソース競合およびサービスの低下を防ぐことによってサービスの品質を確保できます。テナントが他のすべてのテナントのシステム・パフォーマンスに悪影響を及ぼす可能性がある何テラバイトものデータを照会するのを防止できます。

MSSP として、各テナントが比較される一連の基準に基づいて標準のリソース制限を定義できます。例えば、中規模テナントの標準構成に、検索で過去 14 日間のデータにのみアクセスし、最大で 10,000 件のレコードが返されるように制限するリソース制限を含めることができます。

分散環境でのリソース制限

分散環境では、IBM Security QRadar コンソールと管理対象ホストの間でのデータ転送のタイミングによっては、検索結果に影響が及ぶ可能性があります。

IBM Security QRadar で検索を実行すると、検索はすべてのノードで同時に実行されます。各管理対象ホストで検索が実行され、検索が完了するか定義済みの行数に到達すると、集約された結果が QRadar コンソールに送信されます。

以下のように、設定するリソース制限によって、ユーザーに返される検索結果にどのように影響が及ぶ可能性があるのかを理解することが重要です。

キャンセルされた検索

各管理対象ホストは、リソース制限の限度の状態を定期的に検査します。限度に達した場合、不完全な結果がキャッシュおよび再使用されないように、検索が自動的にキャンセルされます。

システムが検索をキャンセルするまでに収集された結果は、「ログ・アクティビティー」タブまたは「ネットワーク・アクティビティー」タブで「検索」 > 「検索結果の管理」をクリックすることにより表示できます。

空の検索結果

時間制限またはレコード制限の制限を設定した場合、管理対象ホストが部分的な集約を QRadar コンソールに送信する前に、リモートの集約によってコンソールがリソース制限の限度に達する可能性があります。この場合、一部のデータが収集されていても、検索結果には何も表示されない可能性があります。

矛盾する検索結果

QRadar は、各管理対象ホストの負荷をモニターし、デプロイメント全体を通して最適化されたパフォーマンスが確保されるように検索を管理します。

システム負荷によっては、繰り返し実行される検索で、多少異なる結果が示される可能性があります。これは、複数の管理対象ホストが異なる順序でデータを返すためです。

例えば、6 個のイベント・プロセッサーが存在するデプロイメントにおいて、EP1、EP3、および EP5 が 1 回目の実行でデータを返す最初のプロセッサーである場合を考えます。その後の実行で、EP2、EP4、および EP6 が最初にデータを返す可能性があり、これが矛盾した検索結果の原因になります。

ユーザーがリソース制限に達する頻度に応じて、ユーザーが業務上の要件を満たすために正当な検索を実行することを制限しないように限度を調整することができます。システムに負担をかける検索を連続して実行するユーザーの場合、QRadar 照会のビルドに関するトレーニングをさらに行うことによって利益を享受できる可能性があります。詳しくは、「*IBM Security QRadar Ariel* 照会言語ガイド」を参照してください。

リソース制限の構成

リソース制限を設定して、イベントおよびフローの検索に対する時間またはデータの制限を適用します。

このタスクについて

以下のタイプのリソース制限を設定することができます。

- データを返すまでの照会の最大実行時間を指定するには、「実行時間」の制限を設定します。
- 検索照会によって返すデータ・レコードの最大数を指定するには、「レコード制限」の制限を設定します。
- 検索対象データの時間幅を指定するには、「時間幅」の制限を指定します。

リソース制限によって制限されている検索を実行するユーザーには、検索条件の横にリソース制限アイコン () が表示されます。

手順

1. 「管理」タブをクリックします。
2. ナビゲーション・メニューで、「システム構成」 > 「リソース制限」をクリックします。
3. デプロイメント内に構成されたテナントが存在する場合は、「ロール」または「テナント」をクリックして、設定する制限のタイプを指定します。
4. 制限の設定対象のロールまたはテナントをダブルクリックします。
5. ユーザー・ロールまたはテナントに割り当てられているすべてのユーザーに対して制限を設定するには、以下の手順に従います。
   a. 上部にあるサマリーの行をクリックして、「制限の編集」ダイアログ・ボックスを開きます。
   b. 設定する制限のタイプについて「有効」をクリックし、制限値を指定します。

c. 「保存」をクリックします。

6. 特定のユーザーに対する制限を設定するには、以下の手順に従います。
   a. 制限を設定するユーザーをダブルクリックします。 ユーザーを検索する場合は、フィルター・フィールドにユーザー名を入力します。
   b. 設定する制限のタイプについて「有効」をクリックし、制限値を指定します。
   c. 「保存」をクリックします。

アプリケーション・ノード

アプリケーション・ノードをプロビジョンすることで、QRadar コンソールの処理能力に影響を与えずに、アプリケーション用の追加のストレージ、メモリー、および CPU リソースを提供します。UBA (User Behavior Analytics) などのアプリケーションは、QRadar コンソールで現在使用できるリソースより多くのリソースを必要とします。

QRadar の「管理」タブで「ノード管理」ウィンドウを使用してアプリケーション・ノードをインストールします。RHEL 7.3 または CentOS 7.3 を実行している任意のコンピューターをアプリケーション・ノードとして使用できます。ノードのセットアップ・プロセスでは、必要なすべてのソフトウェアがインストールおよび構成されます。 QRadar コンソールにインストールされているアプリケーションは、アプリケーション・ノードを追加する際にアプリケーション・ノードに移動されます。

注: QRadar の管理対象ホストをアプリケーション・ノードとして使用することはできません。アプリケーション・ノードには外部ホストを使用する必要があり、1 つの QRadar デプロイメントに使用できるアプリケーション・ノードは 1 つのみです。

関連概念:

224 ページの『アプリケーションのバックアップとリストア』

IBM Security QRadar には、アプリケーション・データとは別に、アプリケーションの構成をバックアップおよびリストアするための方法が用意されています。

アプリケーション・ノードのセットアップ概要

アプリケーション・ノード・サーバーをセットアップし、QRadar コンソールからアプリケーション・ノードにアプリケーションを移動するには、いくつかのステップが必要です。

以下に示すステップは、アプリケーション・ノードのセットアップの概要を説明しています。

1. アプリケーション・ノードの要件を満たすホストに Centos 7.3 または RHEL 7.3 の最小構成バージョンをインストールします。

   注: `/store` パーティションに 80% の空きディスク・スペースを確保してください。

2. yum インストール用にパッケージ・リポジトリーを構成します。ローカル DVD ドライブを yum インストール用のパッケージ・リポジトリーにし、マウント・ポイント用のディレクトリーを作成することを検討してください。

   yum repolist コマンドを入力して、リポジトリーが機能していることを確認します。
3. アプリケーション・ノードと QRadar コンソールとの間で日時が同期されていることを確認します。

   timedatectl コマンドを使用して時刻をリセットすることも、**NTP** を構成することもできます。
4. QRadar コンソールにログインし、以下のコマンドを入力して Docker コンテナーをリストします。

   ```
   ls /store/docker/containers/
   ```

   以下のコマンドを入力して、QRadar コンソールのアプリケーションをリストします。

   ```
   /opt/qradar/support/qapp_utils_730.py ps
   ```

   これらのアプリケーションは、アプリケーション・ノードのセットアップを実行する際にアプリケーション・ノードに移動されます。同じコマンドをアプリケーション・ノードで実行し、アプリケーションが移動されていることを確認します。
5. アプリケーション・ノードでアプリケーション・ノード用のユーザー名とパスワードを作成し、そのユーザーに対してパスワードなしの **sudo** アクセス権限を設定します。

   ユーザー名とパスワードをテストし、**sudo** アクセス権限をテストします。
6. アプリケーション・ノードの `/etc/ssh/sshd_config` ファイルで `AllowTcpForwarding` が **yes** に設定されていることを確認します。
7. アプリケーション・ノードの追加手順に従います。アプリケーションを管理するためにアプリケーション・ノードで必要とされるソフトウェアがセットアップ時にインストールされます。アプリケーション・ノードを追加すると、アプリケーション・ノードのホスト名が `control-01` に変わります。
8. QRadar コンソールから移動されたアプリケーションがアプリケーション・ノードで実行されていることを確認します。

アプリケーション・ノードのセットアップ要件

デプロイメント内のアプリケーションの処理の負荷を軽減するために、QRadar コンソールとは別のアプリケーション・ノード・サーバーをセットアップする際は、ご使用のサーバーが最小システム要件 (必要なソフトウェア、開いているポート、オペレーティング・システムのバージョンなど) に準拠していなければなりません。

アプリケーション・ノード・ソフトウェアは、QRadar コンソールからインストールします。QRadar コンソールにインストールされているすべてのアプリケーションは、ノードを初めて追加する際にアプリケーション・ノードに移動されます。

注: SSH やファイアウォールの構成変更など、本書に記載されていないアプリケーション・ノードの構成変更は、アプリケーション・ノードのインストールが失敗する原因となるため、実施しないでください。

物理サーバーまたは VM をアプリケーション・ノードとしてセットアップするには、以下の要件を使用してください。

アプリケーション・ノード・サーバー仕様
: アプリケーション・ノード・サーバーは少なくとも以下の仕様を満たしている必要があります。
  - 12 GB のメモリー
  - 4 つの CPU
  - 256 GB のストレージ

オペレーティング・システム
: オペレーティング・システムは、Red Hat Enterprise Linux (RHEL) 7.3 または CentOS 7.3 でなければなりません。依存関係用のリポジトリーに接続するため、最小構成のインストール・オプションを使用します。

ファイアウォール
: アプリケーション・ノードで `Firewalld` が実行されているようにし、QRadar コンソールがアプリケーション・ノード上のアプリケーションに接続できるようにします。

IPv6 (インターネット・プロトコル・バージョン **6)**
: IPv6 インターネット・プロトコルは Docker の要件であるため、必ずアプリケーション・ノードで実行されているようにします。 IPv4 アドレスを使用している場合は、IPv6 をインターフェースに自動的に割り当てることで、この要件を満たすことができます。IPv6 が実行されていることを確認する簡単な方法は、アプリケーション・ノードのインターフェースで IPv6 アドレスを確認することです。

オペレーティング・システムのリポジトリー
: アプリケーション・ノード・サーバーが RHEL リポジトリーまたは Centos リポジトリーにアクセスできる必要があります。**`yum`** を使用して OS パッケージ依存関係をインストールします。リポジトリーに接続するコマンド、`yum install <package>` を実行し、**`yum`** でのアクセスを検証します。

  注: RHEL インストール用に有効化されたリポジトリーには、`protobuf` RPM (RPM パッケージ・マネージャー) は含まれていません。`protobuf` RPM をインストールするには、optional リポジトリーが有効である必要があります。

  以下のコマンドを入力して optional リポジトリーを有効にします。

  ```
  subscription-manager repos --enable=rhel-7-server-optional-rpms
  ```

  サブスクライブしているリポジトリーをリストするには、以下のコマンドを入力します。

`subscription-manager repos --list`
管理対象ホストとは異なり、アプリケーション・ノードでは、依存関係用のリポジトリーにアクセスする必要があります。このリポジトリーは外部のソースからダウンロードされるため、オペレーティング・システム用に最小構成の ISO をインストールしてもかまいません。この要件は、すべての依存関係が製品インストール・メディアとソフトウェア・フィックスに含まれている管理対象ホストには適用されません。

store パーティション
使用可能なストレージ容量の約 80% を使用する `/store` パーティション。

アプリケーション・ノードのユーザー・アカウント
アプリケーション・ノードで実行されるすべてのコマンドに対し、パスワードなしの **sudo**アクセス権限が付与されたアプリケーション・ノードの専用ユーザー・アカウント。アプリケーション・ノードのユーザー・アカウントにはパスワードがありますが、パスワードなしで操作するために **sudo** を設定します。

QRadar コンソールは、アプリケーション・ノードへの接続にアプリケーション・ノードのユーザー・アカウントとパスワードを使用します。コンソールがアプリケーション・ノードでコマンドを実行する際に、パスワードなしの **sudo** アクセス権限を使用すると効率性が高まります。
root ユーザー・アカウントを使用してアプリケーション・ノードにアクセスすることもできますが、**sudo** を使用するとシステム・セキュリティー監査ログに実行されたコマンドが記録されるため、root ユーザー・アカウントを使用するよりもメリットがあります。

パスワードなしの **sudo** アクセス権限が付与されたユーザー・アカウントを作成する方法について詳しくは、142 ページの『アプリケーション・ノード・ユーザーの作成とパスワードなしの sudo アクセス権限の設定』を参照してください。

タイム・ゾーンの同期
アプリケーション・ノード・サーバーには、QRadar コンソールと同じ時刻およびタイム・ゾーンを設定する必要があります。

QRadar コンソールとアプリケーション・ノードで開くポート
QRadar コンソールからアプリケーション・ノードへの外部ファイアウォールのポート 1443 と 5443 が開いている必要があります。

アプリケーション・ノードから QRadar コンソールに戻るすべての外部ファイアウォールでポート 5443 と 5444 が開いている必要があります。

QRadar コンソールとアプリケーション・ノードの間の暗号化トンネル
アプリケーション・ノード・サーバーと QRadar コンソールの間に暗号化トンネルを設定することはできません。

アプリケーション・ノード・ユーザーの **umask** 値
アプリケーション・ノード・ユーザーのデフォルト umask 値を 0022 から変更してはなりません。異なる umask 値を使用すると、アプリケーション・ノードの一部のファイルやディレクトリーに対するユーザーの読み取り権限、書き込み権限、実行権限、および検索権限が変更され、正しく機能しなくなる原因となる恐れがあります。**umask** コマンドを使用して、アプリケーション・ユーザーの umask 値を確認します。

連邦情報処理標準 **(FIPS)**
: アプリケーション・ノード・サーバーは、連邦情報処理標準 (FIPS) モードでは機能しません。

QRadar コンソールとアプリケーション・ノードのパフォーマンス
: 最適なパフォーマンスを得るには、アプリケーション・ノード・サーバーと QRadar コンソールを同じデータ・センター内に配置します。

ネットワーク・アドレス変換 **(NAT)**
: ネットワーク・アドレス変換 (NAT) を使用する環境の場合、QRadar コンソールとアプリケーション・ノードの両方が同じ NAT グループ内に存在している必要があります。

TCP 転送
: /etc/ssh/sshd_config ファイルの **AllowTcpForwarding** パラメーターがデフォルトの設定値である yes に設定されていることを確認します。

  /etc/ssh/sshd_config ファイル内の以下のいずれかのエントリーが許容されます。

```
AllowTcpForwarding yes
```

```
#AllowTcpForwarding yes
```

  注: **AllowTcpForwarding** パラメーターが no に設定されている場合、アプリケーション・ノードのインストールは失敗します。

アプリケーション・ノードと **Web** プロキシーの構成
: アプリケーション・ノードが Web プロキシーを使用するように構成されている場合、/etc/environment ファイルに NO_PROXY 構成を追加し、consul.service.consul や vault.service.consul などのサービスと localhost が Web プロキシーへの呼び出しを行わないようにする必要があります。

  /etc/environment ファイルに以下の行を (一行で) 追加します。

```
NO_PROXY="<IP_Address_app_node_host>,
localhost,127.0.0.1,zookeeper.service.consul,vault.service.consul,
docker-registry.service.consul,marathon.service.consul,
consul.service.consul,framework_app_proxy.service.consul,
service-launcher.service.consul"
```

関連タスク:

144 ページの『アプリケーション・ノードの追加』

アプリケーションに対して QRadar コンソールによって実行される処理能力を補うには、アプリケーション・ノードをデプロイメント環境に追加します。アプリケーション・ノードは、アプリケーションの実行専用の非管理対象ホストです。QRadar コンソールの「管理」タブ内の「ノード管理」ウィンドウを使用して、アプリケーション・ノードを追加します。

アプリケーション・ノード・ユーザーの作成とパスワードなしの sudo アクセス権限の設定

アプリケーション・ノードのユーザーとパスワードを作成し、そのアプリケーション・ノード・ユーザーに対してパスワードなしの sudo を設定して、効率性とセキュリティーを向上させます。

手順

1. 以下のコマンドを入力してアプリケーション・ノード・ユーザーを作成します。

   ```
   useradd <app_node_user>
   ```

   ```
   passwd <app_node_user>
   ```

2. visudo を入力して /etc/sudoers ファイルを編集し、ファイルの末尾に以下の行を追加します。

   ```
   <app_node_user> ALL=(ALL) <tab> NOPASSWD: ALL
   ```

   sudoers ファイルには、sudo コマンドを使用する際にユーザーが従う必要のあるルールが記載されています。

3. ファイルを保存して閉じます。

アプリケーション・ノードのセットアップのヘルプ

Docker やアプリケーションの状況をリストしたり確認したりするために、セットアップ時には QRadar コンソールで、セットアップの終了時にはアプリケーション・ノードでさまざまなコマンドを使用できます。

以下に、アプリケーション・ノードのセットアップを支援し、アプリケーションの状況を確認するために使用できる便利なコマンドをリストします。

アプリケーション・ノードでパスワードなしの **sudo** が機能することを検証する

例: sudo cat /etc/hosts

root ユーザー・アカウントを使用して **sudo** アクセス権限をテストするには、以下のコマンドを入力します。
sudo -u <*appnodeuser*> cat /etc/hosts

QRadar コンソールからアプリケーション・ノードに接続する

Putty などの SSH クライアントを使用して QRadar コンソールからアプリケーション・ノードに接続します。

ssh <*app_node_user*>@<*app_node_IP_Address*>

例: ssh appnodeuser@172.16.2.2
アプリケーション・ノードに次のようなプロンプトが表示されます:
[appnodeuser@control-01 ~]$ または [root@control-01 ~]$ (root ユーザーでログインした場合)。

アプリケーションをリストする

QRadar コンソールで /opt/qradar/support/ ディレクトリーに移動し、以下のコマンドを入力してインストール済みアプリケーションをリストします。

qapp_utils_730.py ps

以下に、QRadar コンソールの /opt/qradar/support/ ディレクトリーからコマンドを実行した場合の例を示します。

[root@my_console support]# ./qapp_utils_730.py ps

```
Collecting app data........ Complete!
Id    Name              Container        Container Image     Container ip:port  Host ip:port       ABCDEFGHI
1053  QRadar App Editor 5dca41d9e5e1 qregi...1053:2.0-release 169.254.3.5:5000   9.181.234.86:25568 +++++++++
1054  Hello World -     3455555f3070 qregi.../qapp/1054:1.0.2 169.254.3.6:5000   9.181.234.86:7072 +++++++++
1055  QRadar Vuln app   b79118c4cb0 qregi...44/qapp/1055:1.0  169.254.3.3:5000   9.181.234.86:25600 +++++++++
```

注: アプリケーションがアプリケーション・ノードに移動されると、Host ip:port の参照が QRadar コンソールからアプリケーション・ノードに変わります。

アプリケーション・ノードに **Docker** コンテナーが作成されたことを確認する

アプリケーション・ノードで、以下のコマンドを入力します。

```
ls /store/docker/containers/
```

出力の例を以下に示します。

```
3455555f30703c7641e042e1ddba9c3294174c2d4ed7a0108ef5d9282fcc1d49
364ee70aaee7237676a36ccf007d3664786b6192c545ca328c5512810606fe06
447142c433f59e2937ae4bae2395e23f90db0335deb8287fe6743ca0a864e14b
```

また、アプリケーション・ノードをセットアップする前に、QRadar コンソールでこのコマンドを実行して Docker コンテナーをリストすることもでききます。

Docker サービスが実行されていることを確認する

```
systemctl status docker
```

アプリケーションのコマンド・ラインへのアクセス

アプリケーションのコンテナー ID を使用して、インストール済みアプリケーションのコマンド・ラインにアクセスします。

/opt/qradar/support/qapp_utils_730.py ps コマンドを入力し、実行中のアプリケーション・コンテナーのリストを表示します。次の出力例では、インストールされ、実行されているアプリケーションが示されています。

```
Id      Name    Container         Container Image      Container ip:port   Host ip:port      ABCDEFGHI
1053    QRadar App Editor 5dca41d9e5e1 qregi...1053:2.0-release 169.254.3.5:5000 9.181.234.86:25568 +++++++++
```

以下のコマンドを入力してアプリケーションに接続します。

/opt/qradar/support/qapp_utils_730.py connect <*app_ID*>
出力の例を以下に示します。

```
Collecting app data........ Complete!
bash-4.1#
```

/store ディレクトリーに移動してアプリケーション・ログを表示します。

```
bash-4.1# ls
app           celery_worker  etc   lib64  proc     sbin                    src_deps            store          usr
app_template  celeryd.conf   home  media  qpython  secret_env_unwrap.sh    srv                 sys            var
bin           dev            init  mnt    root     selinux                 start_container.sh  tmp
boot          dump.rdb       lib   opt    run.py   service_port_locator.py  start_flask.sh      upgradePath.sh
bash-4.1# cd store
bash-4.1# ls
log
bash-4.1# cd log
bash-4.1# ls
app.log  celery.log  startup.log  supervisord.log
bash-4.1#
```

アプリケーション・ノードの追加

アプリケーションに対して QRadar コンソールによって実行される処理能力を補うには、アプリケーション・ノードをデプロイメント環境に追加します。アプリケーション・ノードは、アプリケーションの実行専用の非管理対象ホストです。QRadar コンソールの「管理」タブ内の「ノード管理」ウィンドウを使用して、アプリケーション・ノードを追加します。

始める前に

アプリケーション・ノードを追加するには、その前に以下を行います。

- ネットワーク上に Red Hat Enterprise Linux バージョン 7.3 または CentOS バージョン 7.3 が稼働するホストをインストールする必要があります。
- ホストの IP アドレスと **sudo** アクセス権限を持つユーザー・アカウントを指定する必要があります。

アプリケーション・ノードとして動作するようにサーバーをセットアップする方法について詳しくは、139 ページの『アプリケーション・ノードのセットアップ要件』を参照してください。

このタスクについて

手順

1. 「管理」タブで、「ノード管理」をクリックします。
2. アプリケーション・ノードを追加するには、「ノード管理」ウィンドウで「追加」をクリックし、ノード IP アドレス、ユーザーおよびパスワードの情報を追加します。

   その後、本製品で、作成しているノードのホスト **ssh** 鍵情報を確認する必要があります。インストール・プロセスが完了するのに最長で 30 分かかります。実行中のインストール・プロセスについて詳しくは、「詳細」をクリックしてください。

   アプリケーション・ノードのセットアップ・プロセスは、QRadar コンソールにインストールされたすべてのアプリケーションをアプリケーション・ノードに移動します。

   注**:** アプリケーション・ノードは、アプリケーションの移動時に、QRadar コンソール上で実行中または停止されていたすべてのアプリケーションの状況を実行中状態に変更します。

次のタスク

「拡張の管理」ウィンドウを使用して、セットアップしたアプリケーション・ノードにアプリケーションをインストールします。今後インストールされるアプリケーションはすべて、QRadar コンソールではなく、アプリケーション・ノードにインストールされます。

アプリケーション・ノードの削除

サーバーの保守または統合を行っている場合、デプロイメント環境からアプリケーション・ノードを削除できます。アプリケーション・ノードを削除するには、「管理」タブの「ノード管理」ウィンドウを使用します。

手順

「ノード管理」ウィンドウで、「ノード管理」表内の削除するノードを選択し、「削除」をクリックします。

- アプリケーションをアプリケーション・ノードから QRadar コンソールに戻すには、「コンソールに戻す」削除タイプを選択します。

  本製品は、アプリケーションに使用できるディスク・スペースがある場合、アプリケーションを QRadar コンソールに移動しようとします。アプリケーションの移動順序は、そのサイズ (関連するデータを含む) によって決まります。最も小さいアプリケーションが最初に移動されます。アプリケーションに使用できる QRadar コンソール上のスペースは、アプリケーション・ノード上のスペースより小さい可能性があるため、すべてのアプリケーションを移動できるとは限りません。「コンソールに戻す」削除オプションを選択する前に、「拡張の管理」ウィンドウを使用して、不要になったアプリケーションをアプリケーション・ノードから削除してください。

  デフォルトでは、QRadar コンソール上の使用可能メモリーの 10% まで、および QRadar コンソール上の `/store` パーティションの 90% までがアプリケーションに使用できます。多くのアプリケーション、特に、リソースを多く使用するアプリケーションをコンソールに戻す場合は、アプリケーションに使用できるメモリーをすべて使い切る可能性があります。
- アプリケーション・ノード上でアプリケーションを保持するには、「保守モード **(Maintenance Mode)**」削除タイプを選択します。

  「保守モード **(Maintenance Mode)**」を使用すると、「ノード管理」テーブルからアプリケーション・ノード項目が削除され、アプリケーション・ノード上のアプリケーションが停止します。アプリケーション・ノードを再度追加すると、アプリケーションが再始動します。

進行中の削除プロセスについて詳しくは、「詳細」をクリックしてください。

イベント・ログとフロー・ログの保全性の検査

ログのハッシュが有効なときは、イベント・データとフロー・データを書き込むいずれのシステムでも、ハッシュ・ファイルが作成されます。これらのハッシュ・ファイルを使用して、イベント・ログとフロー・ログが最初にディスクに書き込まれたときから変更されていないことを検査します。

ハッシュ・ファイルは、ハッシュ・ファイルの生成前にイベント・ログとフロー・ログを改ざんできないように、ファイルがディスクに書き込まれる前にメモリー内で生成されます。

始める前に

ご使用の IBM Security QRadar システムで、ログのハッシュが有効になっていることを確認します。フロー・ログ・ハッシュまたはイベント・ログ・ハッシュのパラメーターを有効にする方法について詳しくは、システム設定の構成を参照してください。

このタスクについて

イベントおよびフローのデータ・ストレージがあるシステムにログインし、ユーティリティーを実行してログを検査する必要があります。イベントおよびフローのビューアー・インターフェースでは、ログの保全性を検査できません。

check_ariel_integrity.sh ユーティリティーで使用されるパラメーターについて、次の表で説明します。

表 23. **check_ariel_integrity.sh** ユーティリティーのパラメーター

パラメーター	説明
-d	スキャンするログ・ファイル・データの期間 (分)。この期間は、**-t** パラメーターを使用して指定する終了時刻の直前です。例えば、**-d 5** と入力すると、**-t** の終了時刻より前の 5 分間に収集されたすべてのログ・データがスキャンされます。
-n	スキャンする QRadar データベース。有効なオプションは、events および flows です。
-t	スキャンの終了時刻。終了時刻の形式は、「yyyy/mm/dd hh:mm」です。ここで、hh は、24 時間形式で指定します。終了時刻を入力しない場合、現在の時刻が使用されます。
-a	使用するハッシュ・アルゴリズム。このアルゴリズムは、ハッシュ・キーの作成に使用したのと同じであることが必要です。アルゴリズムを入力しない場合、SHA-1 が使用されます。
-r	ログ・ハッシュの場所。この引数は、構成ファイルで指定されている場所 /opt/qradar/conf/arielConfig.xml にログ・ハッシュがない場合にのみ必要です。
-k	ハッシュ・ベースのメッセージ認証コード (HMAC) 暗号化に使用される鍵。HMAC 鍵を指定しないが、システムで HMAC 暗号化が有効になっている場合、**check_ariel_integrity.sh** スクリプトでは、システム設定で指定されている鍵をデフォルトで使用します。
-h	**check_ariel_integrity.sh** ユーティリティーのヘルプ・メッセージを表示します。

手順

1. SSH を使用して、root ユーザーとして QRadar にログインします。
2. ユーティリティーを実行するには、次のコマンドを入力します。

   ```
   /opt/qradar/bin/check_ariel_integrity.sh -d <duration> -n <database name>
   [-t <endtime>] [-a <hash algorithm>] [-r <hash root directory>] [-k <hmac key>]
   ```

   例えば、イベント・データの最後の 10 分間を検証するには、次のコマンドを入力します。

   ```
   /opt/qradar/bin/check_ariel_integrity.sh -n events -d 10
   ```

タスクの結果

ERROR メッセージまたは FAILED メッセージが返された場合、ディスク上の現在のデータから生成されたハッシュ・キーが、ディスクにデータが書き込まれたときに作成されたハッシュ・キーと一致していません。キーまたはデータが変更されています。

カスタム・アクションの追加

ネットワーク・イベントに応答して特定のアクションを実行するために、カスタム・ルールにスクリプトを添付します。「カスタム・アクション」ウィンドウを使用して、カスタム・アクション・スクリプトを管理します。

カスタム・アクションを使用して、スクリプトに渡される値およびその結果実行されるアクションを選択または定義します。

スクリプトに値を渡すことで実行できるカスタム・アクションの例を以下に示します。

- ユーザーおよびドメインのブロック。
- 外部システムでのワークフローおよび更新の開始。
- STIX 形式の脅威による TAXI サーバーの更新。

カスタム・アクションは、低ボリュームのカスタム・ルール・イベントと、応答リミッター値が低いカスタム・ルールで最も適切に機能します。

1. 「管理」タブをクリックします。
2. 「カスタム・アクション」の下の「カスタム・アクションの定義」をクリックします。
3. スクリプトをアップロードするには、「追加」をクリックします。製品でサポートされているプログラミング言語のバージョンが「インタープリター」リストにリストされています。

   デプロイメントのセキュリティーを確保するため、QRadar は、Python、Perl、および Bash 言語で提供されるスクリプト機能の一部をサポートしていません。
4. アップロードしたスクリプトに渡すパラメーターを指定します。

表 24. カスタム・アクション・パラメーター

パラメーター	説明
固定プロパティー	カスタム・アクション・スクリプトに渡される値。 これらのプロパティーはイベントまたはフロー自体に基づくものではありませんが、定義済みのその他の値が、スクリプトを使用したアクションの実行対象に含まれます。 例えば、サード・パーティー・システムの固定プロパティー **username** と **password** をスクリプトに渡して、SMS アラートを送信します。 固定プロパティーを暗号化するには、「暗号化値」チェック・ボックスを選択します。

表 24. カスタム・アクション・パラメーター (続き)

パラメーター	説明
ネットワーク・イベント・プロパティー	イベントにより生成される動的な Ariel プロパティー。「プロパティー」リストから選択します。 例えば、ネットワーク・イベント・プロパティー **sourceip** は、トリガーされたイベントのソース IP アドレスに一致するパラメーターを提供します。 Ariel プロパティーについて詳しくは、「*IBM Security QRadar Ariel* 照会言語ガイド」を参照してください。

パラメーターは、「カスタム・アクションの定義」ダイアログで追加した順でスクリプトに渡されます。

カスタム・アクション・スクリプトが実行されると、/opt/qradar/bin/ca_jail/ ディレクトリー内に chroot jail がセットアップされます。/opt/qradar/bin/ca_jail/ ディレクトリー内の内容はすべて、スクリプトによって変更および書き込みが可能です。カスタム・アクションのユーザーのホーム・ディレクトリー /home/customactionuser) さえも、変更することができます。

スクリプトは jail 環境内部からのみ実行可能であり、QRadar 実行環境は干渉されません。

カスタム・アクションのユーザー・アカウントは、ファイアウォールへのログイン、IP アドレスのブロックなどのフォローアップ・コマンドの実行権限を持っていない可能性があります。スクリプトをルールに関連付ける前に、スクリプトが正常に実行されるかどうかをテストしてください。

注: 実装するカスタム・アクションのタイプは、ネットワーク・インフラストラクチャーとそのコンポーネントによって異なります。例えば、疑わしい IP アドレスをブロックするように Cisco デバイス上で REST API を構成できます。その他のサード・パーティー・ベンダーは REST インターフェースを提供していない可能性があるため、カスタム・アクションを実行するための独自の Web サービス・ソリューションの開発が必要になる場合があります。

カスタム・アクションのテスト

スクリプトをルールに関連付ける前に、スクリプトが正常に実行され、意図した結果になるかどうかをテストします。

このタスクについて

カスタム・アクション・スクリプトは、実稼働環境から分離されたテスト環境内で実行します。カスタム・アクション・スクリプトは通常、イベント・プロセッサーを実行する管理対象ホストで実行されます。ただし、オールインワン・アプライアンスを使用している場合、カスタム・アクションは QRadar コンソールで実行されます。

「テストの実行」は、QRadar コンソールでのみサポートされており、管理対象ホストではサポートされていません。

カスタム・アクション・スクリプトからディスクに書き込みを行う必要がある場合、ディレクトリー /home/customactionuser を使用する必要があります。

手順

1. 「管理」タブで、「アクションの定義」をクリックします。
2. カスタム・アクションをリストから選択し、「テストの実行」 > 「実行」をクリックしてスクリプトをテストします。テストの結果およびスクリプトにより生成される出力 (ある場合) が返されます。
3. カスタム・アクションの構成およびテストが完了したら、「ルール・ウィザード」を使用して、新規イベント・ルールを作成し、それにカスタム・アクションを関連付けます。

   イベント・ルールについて詳しくは、「*IBM Security QRadar* ユーザー・ガイド」を参照してください。

カスタム・アクション・スクリプトへのパラメーターの引き渡し

Bash、Python、および Perl のサンプル・スクリプトは、パラメーターをカスタム・アクション・スクリプトに渡す方法を示しています。

以下のシンプルなサンプル・スクリプトは、アセット・モデル API で指定のオフェンス・ソース IP アドレスを持つアセットを照会する方法を示しています。この例では、便宜上、各スクリプトは、エンドポイントから返される JSON を出力します。

これらのスクリプトには以下の 3 つのパラメーターが必要です。

- コンソール IP アドレス
- API トークン
- オフェンス・ソース IP アドレス

これらのパラメーターは、以下のように、「カスタム・アクションの定義」ウィンドウの「スクリプト・パラメーター」域で構成します。

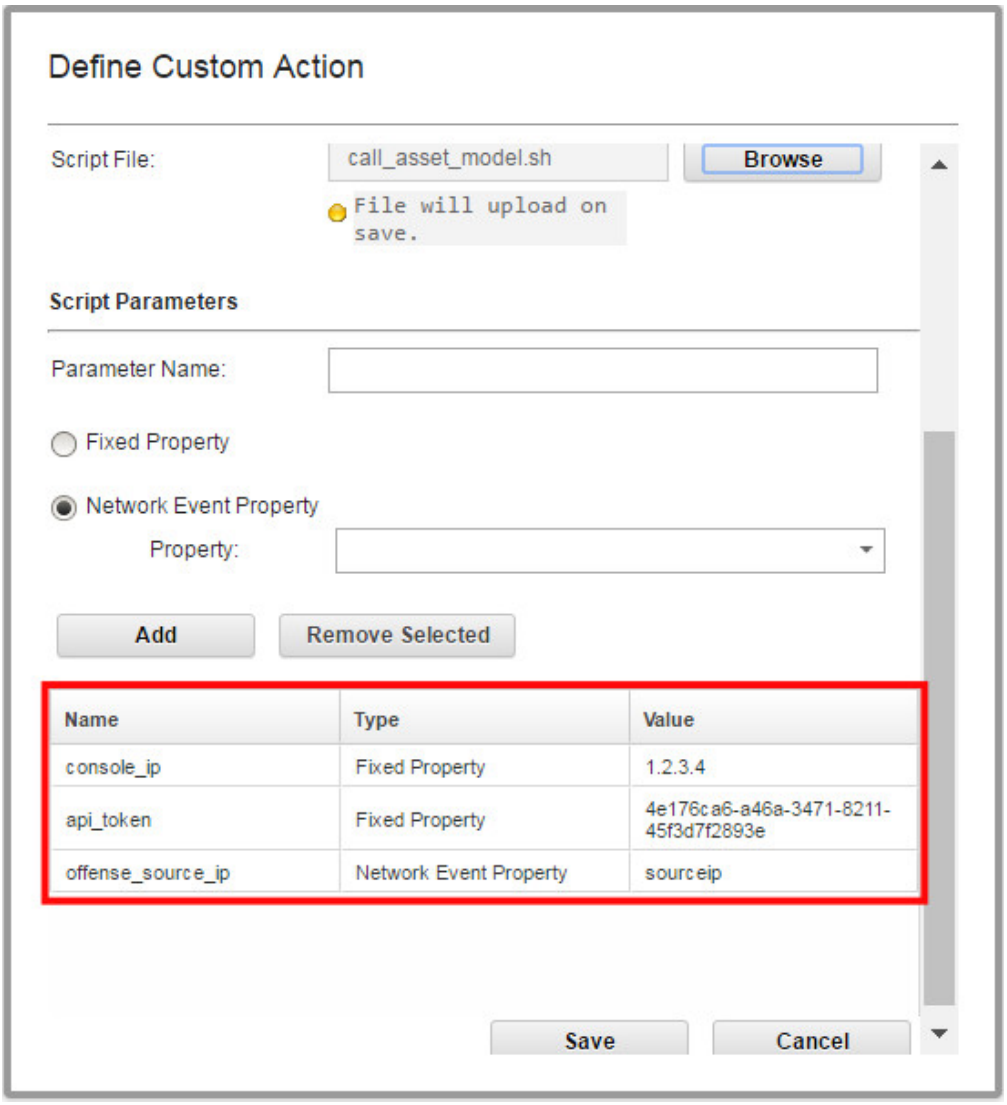


図 3. カスタム・アクション・スクリプトのパラメーター

各パラメーターは、「カスタム・アクションの定義」ウィンドウに追加された順序でスクリプトに渡されます。この場合、以下のようになります。

1. console_ip
2. api_token
3. offense_source_ip

各サンプル・スクリプトの先頭で定義されている変数は、「カスタム・アクションの定義」ウィンドウで追加されたサンプル・パラメーター名を使用します。

```
#!/bin/bash
console_ip=$1
api_token=$2
offense_source_ip=$3

auth_header="SEC:$api_token"

output=$(curl -k -H $auth_header https://$console_ip/console/restapi/api/
asset_model/assets?filter=interfaces%20contains%20%28%20ip_addresses
%20contains%20%28%20value%20%3D%20%22$offense_source_ip%22%29%29)

# Basic print out of the output of the command
echo $output
```

図 *4. call_asset_model.sh*

```
#!/usr/bin/python
import sys
import requests
console_ip = sys.argv[1]
api_token = sys.argv[2]
offense_source_ip = sys.argv[3]

auth_header = {'SEC' : api_token }

endpoint = "https://{0}/console/restapi/api/asset_model/
assets?filter=interfaces%20contains%20%28%20ip_addresses
%20contains%20%28%20value%20%3D%20%22{1}%22%29%29"
.format(console_ip, offense_source_ip)

response = requests.get(endpoint, headers=auth_header, verify=False)

# Basic print out of the output of the command
print(response.json())
```

図 *5. call_asset_model.py*

```
#!/usr/bin/perl
use strict;
use warnings;
use LWP::UserAgent;

my $console_ip = $ARGV[0];
my $api_token = $ARGV[1];
my $offense_source_ip = $ARGV[2];

my $endpoint = "https://$console_ip/console/restapi/api/asset_model/
assets?filter=interfaces%20contains%20%28%20ip_addresses
%20contains%20%28%20value%20%3D%20%22$offense_source_ip%22%29%29";

my $client = LWP::UserAgent -> new(ssl_opts => { verify_hostname => 0 });

my $response = $client -> get($endpoint, "SEC" => $api_token);

# Basic print out of the output of the command
print $response -> decoded_content;
```

図 *6. call_asset_model.pl*

集約データ・ビューの管理

大容量データの集計は、システム・パフォーマンスを低下させる可能性があります。Ariel の関数は、システム・パフォーマンスを改善してデータをより簡単に使用できるようにするため、集約データに対して別個のデータベースを使用します。集約データ・ビューの無効化、有効化、削除が実行できます。時系列グラフ、レポート・グラフ、およびアノマリ・ルールは、集約データ・ビューを使用します。

このタスクについて

「表示」リストに表示される項目は、データをソートします。

集約データ・ビューは、ADE ルール、時系列グラフ、およびレポートのためのデータを生成するために必要です。

ビューの最大数に到達したら、ビューを無効にするか、削除します。

集約データ・ビューには複数の検索が含まれていることがあるため、「集約データ **ID**」列に重複するビューが表示されることがあります。

手順

1. 「管理」タブで、「システム構成」をクリックします。
2. 「集約データ管理」アイコンをクリックします。
3. 集約データ・ビューのリストをフィルタリングするには、次のいずれかのオプションを実行します。
   - 「ビュー」、「データベース」、「表示 **(Show)**」、または「表示」リストからオプションを選択します。
   - 検索フィールドに、集約データ ID、レポート名、グラフ名、または保存済み検索名を入力します。
4. 集約データ・ビューを管理するには、そのビューを選択し、ツールバーで該当するアクションをクリックします。
   - 「ビューの無効化」または「ビューの削除」を選択した場合、集約データ・ビューのコンテンツの依存関係が表示されます。ビューを無効にするか、削除した後は、依存コンポーネントが集約データを使用できなくなります。
   - 以前に無効にした集約データ・ビューをリストアするには、そのビューを有効にします。

表 *25.* 「集約データ管理」ビューの列の説明

列	説明
集約データ ID	集約データの ID
保存済み検索名	保存済み検索に対して定義された名前
列名	列 ID
検索数 (Times Searches)	検索カウント
書き込まれたデータ	書き込まれたデータのサイズ
データベース名	ファイルが書き込まれたデータベース
最終変更時刻	データの最終変更のタイム・スタンプ

表 25. 「集約データ管理」ビューの列の説明 (続き)

列	説明
有効な固有の数	True または False。結果を検索して、経時的な平均数ではなく、固有のイベントとフローの数を表示します。

GLOBALVIEW データベースへのアクセス

QRadar REST API 資料インターフェースを使用して、指定した保存済み検索名および時刻範囲の GLOBALVIEW データベース結果を取得します。データベース結果に含まれるデータのタイプは、照会した保存済み検索のタイプと一致します。

手順

1. 保存済み検索を見つけます。
   a. 「管理」タブで、「集約データ管理」をクリックします。
   b. 「保存済み検索名」列の下で、リストから保存済み検索名を記録します。
2. QRadar REST API を照会して、検索 ID を見つけます。
   a. QRadar API (`https://<Console IP>/api_doc`) に管理者としてログインします。
   b. 最新バージョンの QRadar API をクリックします。
   c. `/ariel/searches` エンドポイントをクリックします。
   d. 「**POST**」をクリックします。
   e. **`query_expression`** パラメーター・フィールドで、以下のコマンドを入力します。 `select * from GLOBALVIEW('savedsearch','timerange')`

      timerange 変数に以下の値のいずれかを使用します。

      NORMAL
      HOURLY
      DAILY

      以下の例は、時刻範囲が過去 2 日の上位ログ・ソースの照会を示しています。

      ```
      select * from GLOBALVIEW('Top Log Sources','DAILY') last 2 days
      ```

   f. 「試用」をクリックします。
   g. 応答本体から検索 ID をコピーします。
3. 検索結果を取得します。
   a. `/ariel/searches/search{id}/results` エンドポイントから、「**GET**」をクリックします。
   b. **`search_id`** パラメーター・フィールドに、検索 ID を入力します。
   c. 「試用」をクリックします。
   d. 検索が正常に完了したことを確認します。
   e. 応答本体からデータベース結果を取得します。

第 7 章 QRadar でのイベント・データの処理

IBM Security QRadar では、DSM エディターを使用して、構文解析の問題を解決したり、カスタム構文解析を追加したりします。

DSM エディターには、カスタマイズが予期したように動作するかどうか判別するためのリアルタイム・フィードバックが備わっています。

関連概念:

5 ページの『IBM Security QRadar 製品の機能』
IBM Security QRadar 製品資料では、オフェンス、フロー、アセット、ヒストリカル相関などの機能について説明していますが、すべての QRadar 製品でこれらの機能を利用できるわけではありません。使用する製品によっては、説明されている一部の機能をデプロイメントで使用できない場合があります。各製品の機能を確認して、必要な情報を入手してください。

DSM エディターの概要

解析時の問題を修正するため、または新規ログ・ソース・タイプのサポートを拡張するためにログ・ソース拡張を手動で作成する代わりに、DSM エディターを使用します。DSM エディターはデータのさまざまなビューを提供します。DSM エディターを使用して、フィールドの抽出、カスタム・プロパティーの定義、イベントのカテゴリー化、および新規 QID 定義を行います。

DSM エディターには以下のビューが備わっています。

ワークスペース

「ワークスペース」には生のイベント・データが表示されます。サンプルのイベント・ペイロードを使用して、ログ・ソース・タイプの振る舞いをテストすると、キャプチャーするデータが「ワークスペース」領域にリアルタイムに表示されます。

すべてのサンプル・イベントがワークスペースから DSM シミュレーターに送信されます。DSM シミュレーターでは、プロパティーの解析と QID マップのルックアップが実行されます。結果は、「ログ・アクティビティーのプレビュー」セクションに表示されます。鉛筆アイコンをクリックして編集モードで開きます。

編集モードの場合、イベント・データをワークスペースに貼り付ける (最大 100,000 文字) か、データを直接編集します。「プロパティー」タブでのプロパティーの編集時は、ペイロード内の一致がワークスペース内で強調表示されます。カスタム・プロパティーおよびオーバーライドされたシステム・プロパティーも、「ワークスペース」内で強調表示されます。

ログ・アクティビティーのプレビュー

「ログ・アクティビティーのプレビュー」では、ワークスペース内のペイロードが「ログ・アクティビティー」ビューアーにどのように表示されるかをシミュレートします。サポートされている標準プロパティーがすべて表示されます。アスタリス

ク (*) のマークが付いたフィールド (例: **イベント名**、**重大度**、**下位カテゴリー**、および「**QID**」) に QID マップからデータが取り込まれます。QID マップからデータが取り込まれるフィールドは、ワークスペース内の生のイベント・データから字句どおりに解析できないため、定義することも編集することもできません。ただし、それらの値は、「イベント・マッピング」タブで対応するイベント ID とカテゴリーの組み合わせを選択することで、調整できます。

レンチ・アイコンをクリックして、「ログ・アクティビティーのプレビュー」ウィンドウで表示または非表示にする列の選択および列の再配列を行います。

プロパティー

「プロパティー」タブには、DSM の構成の要素であるカスタム・プロパティーとシステム・プロパティーを組み合わせたセットがあります。システム・プロパティーの構成はカスタム・プロパティーの構成とは異なります。プロパティーをオーバーライドするには、「システム動作のオーバーライド」チェック・ボックスを選択して、正規表現およびフォーマット・ストリングを入力します。

ペイロード内の一致はワークスペースのイベント・データ内で強調表示されます。この強調表示の色は、キャプチャーするデータに応じて、ツートンカラーとなります。例えば、オレンジ色の強調表示はキャプチャー・グループの値を表し、明るい黄色の強調表示は、ユーザーが指定したその他の正規表現を表します。ワークスペース内のフィードバックは、正規表現が正しいかどうかを示します。式がフォーカスされる場合、ワークスペース内の強調表示は、その式が一致する箇所のみを反映しています。プロパティー全体がフォーカスされる場合、強調表示が緑色になり、一連の式が一致する箇所が優先順位を考慮して示されます。

フォーマット・ストリング・フィールドには、$<数値> 表記を使用してキャプチャー・グループが表されます。例えば、$1 は正規表現からの最初のキャプチャー・グループを表し、$2 は 2 番目のキャプチャー・グループを表すなどです。

同一のプロパティーに複数の式を追加できます。また、式をリストの最上部にドラッグ・アンド・ドロップすることで優先順位を割り当てることができます。

プロパティーの横に警告ツールチップが表示された場合、式が追加されていないことを示します。

「イベント・マッピング」タブ

「イベント・マッピング」タブには、システム内に存在するイベント ID およびカテゴリーのすべての組み合わせが表示されます。新しいイベント・マッピングが作成されると、イベント ID およびカテゴリーの組み合わせのリストに追加されます。このリストは「イベント・マッピング」タブに表示されます。通常、「イベント・マッピング」タブには、イベント ID およびカテゴリーのすべての組み合わせと、それらのマップ先の QID レコードが表示されます。

関連概念:

157 ページの『DSM エディターでのプロパティー』

DSM エディターでは、正規化されたシステム・プロパティーはカスタム・プロパティーと組み合わされ、アルファベット順にソートされます。

DSM エディターでのプロパティー

DSM エディターでは、正規化されたシステム・プロパティーはカスタム・プロパティーと組み合わされ、アルファベット順にソートされます。

DSM では、複数のプロパティーに同じ名前を指定できません。

システム・プロパティーの構成はカスタム・プロパティーの構成とは異なります。

システム・プロパティー

システム・プロパティーは削除することはできませんが、デフォルトの振る舞いをオーバーライドできます。システム・プロパティーには、次の 2 種類があります。

定義済みのシステム・プロパティー

DSM に使用される QRadar のデフォルトの振る舞いが表示されます。

システム・プロパティーのオーバーライド

オーバーライドが構成されているシステム・プロパティー (ログ・ソース拡張) では「状況」行に**「オーバーライド」**が表示されます。システム・プロパティーにオーバーライドが構成されている場合、その DSM のログ・ソース拡張では、構成に入力した正規表現を使用します。

カスタム・プロパティー

カスタム・プロパティーでは「状況」行に**「カスタム」**が表示されます。

カスタム・プロパティーは、システム・プロパティーとは以下の点で異なります。

- カスタム・プロパティーは、名前の下に**「カスタム」**と表示されます。
- カスタム・プロパティーには、「システム動作のオーバーライド」チェック・ボックスがありません。
- ルールおよび検索の索引付けでカスタム・プロパティーを使用できるようにするには、カスタム・プロパティーの作成時に「ルールおよび検索の索引付けでこのプロパティーを使用できるようにする」チェック・ボックスを選択します。

  注**:** このオプションを選択すると、イベントがパイプラインに入るとすぐに QRadar がこのプロパティーをイベントから抽出しようとします。抽出されたプロパティー情報およびその他のイベント・レコードは維持されます。このプロパティーは、検索またはレポートで使用される際に、再び抽出する必要はありません。このプロセスにより、プロパティー取得時のパフォーマンスが向上しますが、イベントの収集と保管時のパフォーマンスに悪影響を及ぼす可能性があります。
- カスタム・プロパティーが有効と見なされるためには、1 つ以上の式が必要です。

関連概念:

155 ページの『DSM エディターの概要』

解析時の問題を修正するため、または新規ログ・ソース・タイプのサポートを拡張するためにログ・ソース拡張を手動で作成する代わりに、DSM エディターを使用します。DSM エディターはデータのさまざまなビューを提供します。DSM エディターを使用して、フィールドの抽出、カスタム・プロパティーの定義、イベントのカ

テゴリー化、および新規 QID 定義を行います。

162 ページの『DSM エディターでのカスタム・プロパティー定義』
カスタム・プロパティーを定義して、別の DSM 内で同じプロパティーを再使用できます。これらのプロパティーを検索やルールで使用すると、それらのフィールドの値を解析するためのユーザー定義の特定の振る舞いが可能になります。

DSM エディターでのプロパティー構成

DSM エディターでプロパティーを構成して、オーバーライド対象のシステム・プロパティーの動作や、DSM のカスタム・プロパティーを変更します。

システム・プロパティーの振る舞いをオーバーライドする場合、「プロパティー構成」タブで、有効な正規表現およびフォーマット設定ストリングを指定する必要があります。**「フォーマット設定ストリング」**フィールドは、正規表現のキャプチャー・グループとリテラル文字を組み合わせたものです。このストリングを使用して、イベントからキャプチャーされた 1 つ以上の値と、追加の書式制御文字や注入された情報がシステム・プロパティーに取り込まれます。例えば、IP アドレスとポートを解析し、この 2 つを組み合わせて 1 つのストリングにすることができます。正規表現 (regex) に 2 つのキャプチャー・グループがある場合、フォーマット・ストリング `$1:$2` を使用してそれらを組み合わせることができます。

重要: DSM エディターでは、いずれの突き合せでも 1 から 9 までのキャプチャー・グループ参照を使用できます。9 より大きい番号のキャプチャー・グループを参照すると、ログ・ソース拡張が正常に機能しない場合があります。

作成するカスタム・プロパティーをそれぞれ構成する必要があります。カスタム・プロパティーの有効な正規表現およびキャプチャー・グループを「プロパティー構成」タブで指定してください。選択度を定義したり、式を有効または無効にしたりすることもできます。

関連概念:

162 ページの『DSM エディターでのカスタム・プロパティー定義』
カスタム・プロパティーを定義して、別の DSM 内で同じプロパティーを再使用できます。 これらのプロパティーを検索やルールで使用すると、それらのフィールドの値を解析するためのユーザー定義の特定の振る舞いが可能になります。

DSM エディターでのフォーマット設定ストリングの作成方法

正規表現で定義したキャプチャー・グループを参照するには、「プロパティー構成」タブの**「フォーマット設定ストリング」**フィールドを使用します。キャプチャー・グループは、優先順位の順序で参照されます。

キャプチャー・グループとは、括弧で囲まれた正規表現のことです。キャプチャー・グループは $n 表記を使用して参照されます。n は、正規表現 (regex) を含むグループ番号です。複数のキャプチャー・グループを定義できます。

例えば、会社変数とホスト名変数を含むペイロードがあるとします。

```
"company":"ibm", "hostname":"localhost.com"
"company":"ibm", "hostname":"johndoe.com"
```

以下のようにキャプチャー・グループを使用して *ibm.hostname.com* を表示するようにペイロードのホスト名をカスタマイズできます。

1. 「**正規表現**」フィールドに以下の正規表現を入力します。

   ```
   "company":"(.*?)".*"hostname":"(.*?)"
   ```

2. 「**フォーマット設定ストリング**」フィールドに、キャプチャー・グループ $1.$2 と入力します。$1 は会社変数の値 (この場合、ibm です) で、$2 はペイロード内のホスト名の値です。

   以下の出力が表示されます。

   ```
   ibm.localhost.com

   ibm.johndoe.com
   ```

適切に構造化されたログの正規表現の作成方法

適切に構造化されたログとは、一連のプロパティーで構成されたイベント・フォーマット設定のスタイルであり、以下のように示されます。

```
<name_of_property_1><assignment_character>
<value_of_property_1><delimiter_character>
<name_of_property_2><assignment_character>
<value_of_property_2><delimiter_character>
<name_of_property_3><assignment_character>
<value_of_property_3><delimiter_character>...
```

以下の一般ガイドラインを使用してください。

- *<assignment_character>* は、「=」または「:」、あるいは「->」などの複数文字からなる文字列です。
- *<delimiter_character>* は、空白文字 (スペースまたはタブ) またはリスト区切り文字 (コンマやセミコロンなど) です。
- *<value_of_property>* と、場合によっては *<name_of_property>* は、引用符または他の囲み文字で囲まれます。

例えば、デバイスやアプリケーションで生成されるシンプルなログイン・イベントについて考えてみます。デバイスが、ログインしたユーザーのアカウント、ログインが発生した時刻、ユーザーのログイン元コンピューターの IP アドレスについて報告するとします。名前/値のペア形式のイベントは、次のスニペットのようになります。

```
<13>Sep 09 22:40:40 9.2.45.12 action=login  accountname=JohnDoe  clientIP=9.21.23.24
timestamp=01/09/2016 22:40:39 UTC
```

注**:** 文字列「<13>Sep 09 22:40:40 9.2.45.12」は Syslog ヘッダーです。この文字列はイベントの本文の一部ではありません。

上記例の適切に構造化されたログのプロパティーをキャプチャーする方法を次の表に示します。

表 *26.* 適切に構造化されたログのプロパティーをキャプチャーするための正規表現

プロパティー	正規表現
action	action=(.*?)¥t
accountname	accountname=(.*?)¥t

表 26. 適切に構造化されたログのプロパティーをキャプチャーするための正規表現 (続き)

プロパティー	正規表現
clientIP	clientIP=(.*?)¥t
timestamp	timestamp=(.*?)¥t

括弧で囲まれたパターンは、キャプチャー・グループを示します。表の各正規表現は、等号 (=) の後から次のタブ文字の前までの間にあるすべてのものをキャプチャーします。

自然言語ログの正規表現の作成方法

自然言語ログは、文章のような形式で示され、イベント・タイプごとに見た目が異なる可能性があります。

例えば、シンプルなログイン・イベントは以下の形式で表示される場合があります。

```
<13>Sep 09 22:40:40 9.2.45.12 Account JohnDoe initiated a login action
from 9.21.23.24 at 01/09/2016 22:40:39 UTC
```

上記例の自然言語ログのプロパティーをキャプチャーする方法を次の表に示します。

表 27. 自然言語ログのプロパティーをキャプチャーするための正規表現

プロパティー	正規表現
action	initiated a (.*?) action
accountname	Account (.*?) initiated
clientIP	from (.*?) at
timestamp	at (.*?)

注: 自然言語ログの正規表現を作成するには、キャプチャー・グループを作成する前に、キャプチャーしたい値を囲む静的情報を確認する必要があります。

DSM エディターを開く

DSM エディターは、「ログ・アクティビティー」タブまたは「管理」タブから開くことができます。

例えば、システムに送信されるイベントが適切に処理されていない場合、そのようなイベント・データを「ログ・アクティビティー」タブで選択して DSM エディターに送信できます。

まだシステムに送信されていないイベントの場合は、管理者が「管理」タブから DSM エディターにアクセスする必要があります。

「管理」タブから DSM エディターを開く

管理者は、「管理」タブから DSM エディターを開くことができます。

手順

1. 「管理」タブをクリックします。
2. ナビゲーション・メニューで、「データ・ソース」 > 「**DSM** エディター」をクリックします。

「ログ・アクティビティー」タブから DSM エディターを開く

QRadar コンソールで受信したイベントを選択することで、「ログ・アクティビティー」タブから DSM エディターを開くことができます。

手順

1. 「ログ・アクティビティー」タブをクリックします。
2. 1 つ以上のイベントを強調表示します。

   重要**:** 複数のログ・ソースから複数のイベントを選択すると、操作するログ・ソース・タイプを選択するよう求めるプロンプトが出されます。選択できるのは、単一のログ・ソース・タイプのみで、選択したログ・ソース・タイプと一致するログ・アクティビティーのイベントのみがワークスペースに自動的に追加されます。
3. ナビゲーション・メニューで、「アクション」 > 「**DSM** エディター」を選択します。

ログ・ソース・タイプの構成

DSM エディターで新しいログ・ソース・タイプを構成することも、IBM Security QRadar の既存のログ・ソース・タイプを使用することもできます。

このタスクについて

サポートされる DSM を持たないカスタム・アプリケーションおよびシステムのログ・ソースを構成することができます。ユニバーサル DSM (uDSM) を使用する代わりに、DSM エディターを使用して新規ログ・ソース・タイプを作成できます。これで、受信イベントおよび追加コンテンツ (カスタムのプロパティー、検索、ルールなど) をそのログ・ソース・タイプのみと関連付けることができます。サポートされる DSM がないすべてのイベント・フィードに対して uDSM を使用すると、関連するコンテンツがすべての該当するイベントに対して実行されます。このようにして uDSM を実行することは、システム・パフォーマンスの観点から望ましくありません。

DSM エディターが機能するのは、一度に 1 つのログ・ソース・タイプに対してのみです。

手順

1. 「管理」タブをクリックします。
2. ナビゲーション・メニューで、「データ・ソース」 > 「**DSM** エディター」をクリックします。
3. ログ・ソース・タイプを作成するか、既存のログ・ソース・タイプを選択します。

- 新しいログ・ソース・タイプを作成するには、「新規作成」をクリックしてプロンプトに従います。
- 既存のログ・ソース・タイプを見つけるには、**「フィルター」**フィールドを使用し、「選択」をクリックします。

DSM エディターでのカスタム・プロパティー定義

カスタム・プロパティーを定義して、別の DSM 内で同じプロパティーを再使用できます。これらのプロパティーを検索やルールで使用すると、それらのフィールドの値を解析するためのユーザー定義の特定の振る舞いが可能になります。

関連性がある場合、各カスタム・プロパティーには一連の構成オプション (選択度、データの構文解析を含む) があります。DSM の構成内にある各カスタム・プロパティー定義は、複数の式の順序付けされたグループです。このグループは、正規表現、キャプチャー・グループ、選択度構成 (オプション)、および有効/無効のトグル・ボタンで構成されます。DSM エディターの「プロパティー」タブ内にあるカスタム・プロパティーの**「名前」**、**「フィールド・タイプ」**、**「説明」**、**「最適化 (optimize)」**の各フィールド、およびカスタム・プロパティーのすべての詳細オプションは変更できません。

カスタム・プロパティーはすべての DSM で共有されるのに対して、ペイロードからの値の読み取りに関する特定の実装は DSM レベルで行います。

特定の条件が満たされた場合にのみ実行するように式を構成する場合、選択度を指定します。

注**:** カスタム・プロパティーの**「キャプチャー・グループ」**フィールドに、正規表現でのキャプチャー・グループの数より大きい値を割り当てることはできません。

関連概念:

157 ページの『DSM エディターでのプロパティー』

DSM エディターでは、正規化されたシステム・プロパティーはカスタム・プロパティーと組み合わされ、アルファベット順にソートされます。

選択度

DSM エディターでは、パフォーマンス向上のために、カスタム・プロパティーの実行を特定の条件に制限することができます。

制限のタイプを以下に示します。

上位カテゴリーおよび下位カテゴリーによる制限
: 上位カテゴリーおよび下位カテゴリーが特定の組み合わせに一致する場合にのみ、プロパティーが評価されます。例えば、イベントに**「認証」**の上位カテゴリーおよび**「管理者のログアウト」**の下位カテゴリーがあると認識した場合にのみプロパティーが評価されます。

特定の **QID** による制限
: 表示されたイベントが特定の QID にマップされている場合にのみプロパティーが評価されます。例えば、イベントが**「ログイン失敗」**の QID にマップされている場合にプロパティーが評価されます。

式

DSM エディターでカスタム・プロパティーの式を定義できます。式は、プロパティーの振る舞いを定義する手段です。式の主な構成要素は、有効な正規表現です。式を構成するデータはプロパティー・タイプによって異なります。

カスタム・プロパティーの場合、正規表現の 1 つのキャプチャー・グループのみを選択できます。

カスタム・プロパティーの作成

DSM エディターでは、IBM Security QRadar の正規化イベント・モデルに適合しないイベントがある 1 つ以上のログ・ソースについて、カスタム・プロパティーを定義できます。例えば、システム・プロパティーでは、一部のアプリケーション、オペレーション・システム、データベース、その他のシステムのデータをキャプチャーできない場合があります。

このタスクについて

QRadar のシステム・プロパティーに適合しないデータに対して、カスタム・プロパティーを作成できます。検索でカスタム・プロパティーを使用して、ルールでそれらのテストを行うことができます。

手順

1. カスタム・プロパティーを追加するために、DSM エディターの「プロパティー」タブで追加 (+) アイコンをクリックします。
2. 新規カスタム・プロパティー定義を作成するには、以下の手順を実行します。
   a. 「表現するカスタム・プロパティー定義の選択」ページで「新規作成」を選択します。
   b. 「新規カスタム・プロパティー定義の作成」ページで、**「名前」**、**「フィールド・タイプ」**、および**「説明」**の各フィールドに値を入力します。
   c. イベントがシステムで開始されるときにイベントのプロパティーを抽出するには、「ルールおよび検索の索引付けでこのプロパティーを使用できるようにする」チェック・ボックスを選択します。
   d. 「保存」をクリックします。
3. 既存のカスタム・プロパティーを使用するには、以下の手順を実行します。
   a. 「表現するカスタム・プロパティー定義の選択」ページの**「フィルター定義」**フィールドで、既存のカスタム・プロパティーを検索します。
   b. 「選択」をクリックしてカスタム・プロパティーを追加します。
4. カスタム・プロパティーを構成するには、以下の手順を実行します。
   a. 「プロパティー」タブでカスタム・プロパティーを見つけて選択します。システム・プロパティーと区別するために、カスタム・プロパティーの横には、**「カスタム」**と表示されています。
   b. カスタム・プロパティーの正規表現を定義し、キャプチャー・グループを選択します。
   c. カテゴリーのレベルを割り当てるために、「編集」をクリックしてカスタム・プロパティーに選択度を追加し、「上位カテゴリー」および「下位カテゴリー」を選択します。

d. 新しいイベント・カテゴリー化を作成するために、「選択度」ウィンドウで「イベントの選択」をクリックします。
e. 「イベント・カテゴリー化」ウィンドウで、「新しい **QID** レコードの作成」をクリックします。
f. 「名前」、「説明」を入力し、「ログ・ソース・タイプ」、「上位カテゴリー」、「下位カテゴリー」、および「重大度」を選択します。
g. 「保存」をクリックします。
h. 「イベント・カテゴリー化」ウィンドウで、新しく作成した QID を選択し、「**OK**」をクリックします。
i. 「式」ウィンドウで、「**OK**」をクリックします。

5. 複数の式を追加してそれらの順序を変更するには、次の手順に従います。
a. 式リストの最上部にある追加 (+) アイコンをクリックします。
b. 式をドラッグ・アンド・ドロップして、実行する順序に並べ替えます。

イベント・マッピング

DSM エディターで、イベント・マッピングは、システム内に存在するイベント ID およびカテゴリーのすべての組み合わせを示します。

イベント・マッピングは、イベント ID およびカテゴリーの組み合わせと QID レコード (イベント・カテゴリー化と呼びます) の間の関連付けを表します。イベント ID およびカテゴリーの値は、DSM によってイベントから抽出され、マップされているイベント・カテゴリー化または QID の検索に使用されます。イベント・カテゴリー化によって、生のイベント・データに字句どおりに存在しない可能性があるイベントの追加のメタデータ (人間が理解できる名前や説明、重大度値、下位カテゴリーの割り当てなど) が保管されます。下位カテゴリー化および重大度は、検索およびルール定義で役立ちます。

注**:** マルチテナント環境の場合、DSM エディターで定義したユーザー定義のマッピング情報やイベント・カテゴリー化情報は、すべてのテナントに対して可視になります。テナント固有のデータがイベント・カテゴリー化の名前または説明に含まれることがないようにしてください。

イベント・マッピングのためのアイデンティティー・プロパティー

アイデンティティー・データとは、システム・プロパティーの特殊なセットです。これらのプロパティーには、アイデンティティー・ユーザー名、アイデンティティー **IP**、アイデンティティー **NetBIOS** 名 **(Identity NetBIOS Name)**、アイデンティティー拡張フィールド、アイデンティティー・ホスト名、アイデンティティー **MAC**、アイデンティティー・グループ名などがあります。

DSM によってアイデンティティー・プロパティーにデータが取り込まれると、IBM Security QRadar コンソールで実行されるアセット・プロファイラー・サービスにアイデンティティー・データが転送されます。アセット・プロファイラーは、新規アセットの追加または既存アセットの情報 (アイデンティティー・ユーザー名が指定されている場合はアセット・フィールド「最後のユーザー」および「最後に確認されたユーザー」が含まれる) の更新により、アセット・モデルを更新する際に使用されます。

IBM Security QRadar DSM は、アイデンティティー・プロパティー間の関連付けや関連付け解除を確立するイベントなど、特定のイベントのアイデンティティー・データにデータを取り込むことができます。この関連付けや関連付け解除は、パフォーマンスのために行われます。また、アセットの更新に必要な新規の情報や有用な情報を提供する特定のイベントのために行われます。例えば、ログイン・イベントでは、ユーザー名とアセット (IP アドレス、MAC アドレス、ホスト名、またはその組み合わせ) 間の新しい関連付けが確立されます。DSM は、解析したすべてのログイン・イベントのアイデンティティー・データを生成しますが、同じユーザーに関連する後続の別のタイプのイベントでは、新しい関連付けの情報は提供されません。そのため、DSM は別のイベント・タイプのアイデンティティーを生成しません。

また、DHCP サービスの DSM は、DHCP が割り当てられているイベントのアイデンティティー・データを生成する場合があります。このようなイベントによって IP アドレスと MAC アドレス間の関連付けが確立されるためです。DNS ルックアップを表すイベントは IP アドレスとホスト名/DNS 名の間の関連付けを確立するため、DNS サービスの DSM は、このようなイベントのアイデンティティー情報を生成します。

DSM エディターを構成して、アイデンティティー・プロパティーの振る舞いをオーバーライドすることができます。ただし、他のシステム・プロパティーとは異なり、オーバーライドされたアイデンティティー・プロパティーは、イベント ID またはイベント・カテゴリーの特定の組み合わせ (イベント・マッピング) にリンクされていない限り、効果がありません。アイデンティティー・プロパティーのオーバーライドを構成するときは、「イベント・マッピング」タブにアクセスし、イベント・マッピングを選択して、そのイベント用に特定のアイデンティティー・プロパティーを構成できます。イベント用にアイデンティティー・プロパティーにデータが取り込まれるのは、アイデンティティー・プロパティーが使用可能であり、かつ構成済みのプロパティーの正規表現でキャプチャーされる場合のみです。

注: **「アイデンティティー・ユーザー名」**プロパティーは固有であり、かつ独立して構成できません。特定のイベント・マッピング用にアイデンティティー・プロパティーが有効になっている場合、**「アイデンティティー・ユーザー名」**プロパティーには、当該イベント用に**「ユーザー名」**プロパティー値から自動的にデータが取り込まれます。

イベント・マップおよびカテゴリー化の作成

イベント・マッピングは、イベントを QID にマップするために使用する、イベント ID とカテゴリーとの組み合わせです。DSM エディターで新規イベント・マッピングを作成して、すべての不明イベントを QID マップ内のエントリーにマップできます。また、新しく作成されたイベント・カテゴリー化 (QID) とシステムの既存のイベント・カテゴリー化のいずれかに、既存のイベントを再マップできます。

手順

1. イベント・マッピングを追加するために、DSM エディターの「イベント・マッピング」タブで追加 (**+**) アイコンをクリックします。
2. **「イベント ID」**フィールドと**「カテゴリー」**フィールドに値を入力します。
3. 新規イベント・カテゴリー化を作成するには、以下の手順を実行します。

a. 「新規イベント・マッピングの作成」ウィンドウで、「イベントの選択」をクリックします。
b. 「イベント・カテゴリー化」ページで、「新しい **QID** レコードの作成」をクリックします。
c. **「名前」**フィールドと**「説明」**フィールドに値を入力し、**「ログ・ソース・タイプ」**、**「上位カテゴリー」**、**「下位カテゴリー」**、および**「重大度」**を選択します。
d. 「保存」をクリックして、新規イベント・カテゴリー化を作成します。

4. 既存のイベント・カテゴリー化を使用するには、以下の手順を実行します。
a. 「新規イベント・マッピングの作成」ウィンドウで、「イベントの選択」をクリックします。
b. 「イベント・カテゴリー化」ウィンドウで既存のイベント・カテゴリー化を検索します。
c. **「上位カテゴリー」**、**「下位カテゴリー」**、**「ログ・ソース・タイプ」**、または**「QID」**を選択します。結果は「検索結果」ペインに表示されます。
d. 「**OK**」をクリックしてイベント・カテゴリーを追加します。

DSM エディターからのコンテンツのエクスポート

DSM エディター内で作成されたカスタム・コンテンツは、コンテンツ・マネジメント・ツールのスクリプトを使ってエクスポートすることができます。ある IBM Security QRadar デプロイメント環境からコンテンツをエクスポートし、別の QRadar デプロイメント環境にインポートできます。カスタム・コンテンツを外部メディアにエクスポートすることもできます。

DSM エディターでは、以下のコンテンツ・タイプが生成されます。

表 28. DSM エディターのコンテンツ・タイプ

カスタム・コンテンツのタイプ	**String**	**ID**
カスタム・プロパティー	customproperty	6
ログ・ソース・タイプ	sensordevicetype	24
ログ・ソース拡張	deviceextension	16
QidMap のカスタム・エントリー	qidmap	27

contentManagement.pl スクリプトが `/opt/qradar/bin` ディレクトリーにあります。

コンテンツをパッケージとしてエクスポート

コンテンツ管理ツールのスクリプトを使用して、DSM エディターで作成された特定のコンテンツを検索できます。これらのコンテンツはパッケージとしてエクスポートされます。

手順

1. SSH を使用して、root ユーザーとして QRadar にログインします。

2. エクスポートする特定のコンテンツ項目を検索するには、以下のコマンドを入力します。

   ```
   ./contentManagement.pl -a search -c [content_type] -r [regex]
   ```

   例えば、ログ・ソース・タイプのコンテンツ項目を検索するには、以下のコマンドを入力します。

   ```
   /opt/qradar/bin/contentManagement.pl -a search -c 24 -r
   "<search_name>"
   ```

3. エクスポートするコンテンツをリストするテキスト・ファイルを作成します。

   各行に、カスタム・コンテンツ・タイプを入力し、その後にそのタイプの固有 ID のコンマ区切りリストを入力します。

   例えば、ID 24、ID 26、および ID 95 の 3 つのログ・ソース・タイプ (いずれもカスタム・プロパティーです) をエクスポートするには、以下のエントリーを含むテキスト・ファイルを作成します。

   ```
   sensordevicetype, 24,26,95
   ```

4. 以下のコマンドを使用して、コンテンツ項目をパッケージとしてエクスポートします。

   ```
   /opt/qradar/bin/contentManagement.pl -a export -c package -f <source_file>
   ```

単一のカスタム・プロパティーのコンテンツのエクスポート

コンテンツ管理ツールのスクリプトを使用して、DSM エディターの「プロパティー」タブで作成された各カスタム・プロパティーのコンテンツをエクスポートできます。

このタスクについて

DSM エディターを使用してカスタム・プロパティーを作成すると、作成された各カスタム・プロパティーの **customproperty** エンティティーが生成されます。

手順

1. SSH を使用して、root ユーザーとして QRadar にログインします。
2. エクスポートする特定のコンテンツを検索するには、以下のコマンドを入力します。

   ```
   ./contentManagement.pl -a search -c [content_type] -r [regex]
   ```

   例えば、カスタム・プロパティーのコンテンツを検索するには、以下のコマンドを入力します。

   ```
   /opt/qradar/bin/contentManagement.pl -a search -c 6 -r
   "<name_of_custom_property>"
   ```

3. カスタム・プロパティー・コンテンツをエクスポートするには、以下のコマンドを入力します。

   ```
   /opt/qradar/bin/contentManagement.pl -a export -c [content_type]
   -i [content_identifier]
   ```

第 8 章 QRadar へのリファレンス・データの取得

IBM Security QRadar 環境内のイベントおよびフローに相関させるビジネス・データの保管および管理には、リファレンス・データ収集を使用します。ビジネス・データや外部ソースからのデータをリファレンス・データ収集に追加し、そのデータを QRadar の検索、フィルター、ルール・テスト条件、およびルール応答で使用できます。

リファレンス・データ収集は QRadar コンソールで保管されますが、各管理対象ホストに定期的にコピーされます。データのルックアップで最適なパフォーマンスを得るために、管理対象ホストは最も頻繁に参照されるデータの値をキャッシュに入れます。

外部の脅威インテリジェンス・データ

リファレンス・データ収集を使用して、サード・パーティー・ベンダーから得た IOC (Indicator of Compromise) データを QRadar に統合できます。QRadar は、IOC データを使用して疑わしい振る舞いをより素早く検知し、セキュリティー・アナリストが脅威の調査およびインシデントへの対応をより迅速に行うよう支援します。

例えば、IP アドレス、DNS 名、URL、MD5 などの IOC データを、オープン・ソースまたはサブスクリプションに基づく脅威データのプロバイダーからインポートし、その IOC データを、ご使用のネットワーク内のイベントおよびインシデントに相関させることができます。

ビジネス・データ

リファレンス・データ収集には、所属する組織に固有のビジネス・データ (システムへの特権アクセスを持つユーザーのリストなど) が含まれている可能性があります。ビジネス・データを使用して、ブラックリストおよびホワイトリストを作成します。

例えば、解雇された従業員のユーザー ID を含むリファレンス・セットを使用して、それらの従業員がネットワークにログインするのを防止します。あるいは、一連の限定された IP アドレスのみに特定の機能の実行を許可するホワイトリストを作成するために、ビジネス・データを使用できます。

関連概念:

5 ページの『IBM Security QRadar 製品の機能』
IBM Security QRadar 製品資料では、オフェンス、フロー、アセット、ヒストリカル相関などの機能について説明していますが、すべての QRadar 製品でこれらの機能を利用できるわけではありません。使用する製品によっては、説明されている一部の機能をデプロイメントで使用できない場合があります。各製品の機能を確認して、必要な情報を入手してください。

リファレンス・データ収集のタイプ

さまざまなタイプのリファレンス・データ収集が存在し、それぞれのタイプは、異なるレベルの複雑さのデータを扱うことができます。最も一般的なタイプはリファレンス・セットとリファレンス・マップです。

表 29. リファレンス・データ収集のタイプ

収集のタイプ	説明	使用法
リファレンス・セット	順序性のない、固有値の集合です。 リファレンス・セットを作成するには、QRadar、コマンド・ライン、または RESTful API を使用します。	リファレンス・セットを使用して、IP アドレスやユーザー名などのリストに対してプロパティー値を比較します。 例えば、ログインに使用された **LoginID** がユーザーに割り当てられているかどうかを検証できます。
リファレンス・マップ	1 つの固有のキーを 1 つの値にマップするデータの集合です。 リファレンス・マップを作成するには、コマンド・ラインまたは RESTful API を使用します。	リファレンス・マップを使用して、2 つのプロパティー値の固有の組み合わせを検証します。 例えば、ネットワーク上のユーザー・アクティビティーを相互に関連させるために、**LoginID** パラメーターをキーとして使用し、**Username** パラメーターを値として使用するリファレンス・マップを作成できます。
セットのリファレンス・マップ	1 つのキーを複数の値にマップするデータの集合です。どのキーも固有であり、いずれも 1 つのリファレンス・セットにマップします。 セットのリファレンス・マップを作成するには、コマンド・ラインまたは RESTful API を使用します。	セットのリファレンス・マップを使用して、2 つのプロパティー値の組み合わせをリストに対して検証します。 例えば、ある特許への許可アクセスをテストするために、**Patent ID** のカスタム・イベント・プロパティーをキーとして使用し、**Username** パラメーターを値として使用するセットのマップを作成できます。セットのマップを使用して、許可されたユーザーのリストにデータを取り込みます。
マップのリファレンス・マップ	1 つのキーを別のキーにマップし、その後、このキーが単一値にマップされるデータの集合です。どのキーも固有であり、いずれも 1 つのリファレンス・マップにマップします。 マップのリファレンス・マップを作成するには、コマンド・ラインまたは RESTful API を使用します。	マップのリファレンス・マップを使用して、3 つのプロパティー値の組み合わせを検証します。 例えば、ネットワーク帯域幅の違反が発生していないかをテストするために、1 番目のキーとして **Source IP** パラメーター、2 番目のキーとして **Application** パラメーター、そして値として **Total Bytes** パラメーターを使用するマップのマップを作成できます。

表 29. リファレンス・データ収集のタイプ (続き)

収集のタイプ	説明	使用法
リファレンス・テーブル	マップのマップに似ていますが、2 番目のキーにはデータ・タイプが割り当てられます。 リファレンス・テーブルを作成するには、コマンド・ラインまたは RESTful API を使用します。	プロパティーのいずれかが特定のデータ・タイプである場合、リファレンス・テーブルを使用して、3 つのプロパティー値の組み合わせを検証します。 例えば、1 番目のキーとして **Username**、2 番目のキーとして **Source IP** (割り当てられた **cidr** データ・タイプを持つ)、そして値として **Source Port** を保管するリファレンス・テーブルを作成できます。

QRadar SIEM と QRadar Risk Manager の両方で同じリファレンス・データを使用したい場合は、リファレンス・セットを使用してください。QRadar Risk Manager では、他のタイプのリファレンス・データ収集を使用することはできません。

リファレンス・セット概要

IBM Security QRadar のリファレンス・セットを使用して、単純なリスト形式でデータを保管します。

危殆化を示す痕跡 (IOC) データなどの外部データをリファレンス・セットに取り込むことも、ネットワークで発生したイベントおよびフローから収集されたビジネス・データ (IP アドレス、ユーザー名など) を保管するためにリファレンス・セットを使用することもできます。

リファレンス・セットには、検索、フィルター、ルール・テスト条件、およびルール応答で使用できる固有値が含まれています。ルールを使用してリファレンス・セットにデータ・エレメントが含まれているかテストしたり、データをリファレンス・セットに追加するためのルール応答を構成したりできます。例えば、禁止されている Web サイトにアクセスする従業員を検知するルールを作成し、その従業員の IP アドレスまたはユーザー名をリファレンス・セットに追加するためのルール応答を構成できます。

リファレンス・セットにデータを追加するためのルール応答を構成する方法について詳しくは、「*IBM Security QRadar* ユーザー・ガイド」を参照してください。

リファレンス・セットは、QRadar で管理できる唯一のタイプのリファレンス・データ収集です。コマンド・ラインおよび Restful API 資料インターフェースを使用して、リファレンス・セットを管理することもできます。

関連タスク:

177 ページの『コマンド・ラインを使用したリファレンス・データ収集の作成』
IBM Security QRadar で管理できないリファレンス・データ収集 (リファレンス・マップ、セットのマップ、マップのマップ、テーブルなど) の管理には、コマンド・ラインを使用します。QRadar を使用してリファレンス・セットを管理する方が簡単ですが、管理タスクをスケジュールするときには、コマンド・ラインを使用します。

181 ページの『API を使用したリファレンス・データ収集の作成』
アプリケーション・プログラム・インターフェース (API) を使用して、IBM Security QRadar のリファレンス・データ収集を管理できます。

リファレンス・セットの追加、編集、および削除

リファレンス・セットは、IP アドレスやユーザー名などのプロパティー値をリストに照らして比較するために使用します。リファレンス・セットをルールと共に使用して、ウォッチ・リストを維持できます。例えば、禁止されている Web サイトにアクセスする従業員を検出して、その従業員の IP アドレスをリファレンス・セットに追加するためのルールを作成できます。

このタスクについて

リファレンス・セットにデータを追加すると、「エレメント数」パラメーターと「関連付けられているルール」パラメーターが自動的に更新されます。

リファレンス・セットの編集時に、データ値を変更できますが、リファレンス・セットに格納されるデータのタイプを変更することはできません。

リファレンス・セットが削除される前に、QRadar によって依存関係検査が実行され、リファレンス・セットに関連付けられているルールがないか調べられます。

注**:** リファレンス・セット・データと比較するイベント・プロパティーのデータを難読化する技法を使用する場合、英数字のリファレンス・セットを使用し、難読化されたデータ値を追加します。

手順

1. 「管理」タブで、「リファレンス・セット管理」をクリックします。
2. リファレンス・セットを追加するには、以下の手順を実行します。
   a. 「追加」をクリックし、パラメーターを構成します。

      リファレンス・セットのパラメーターに関する詳細の説明**:**

      以下の表では、リファレンス・セットの構成に使用する各パラメーターについて説明します。

表 *30.* リファレンス・セットのパラメーター

パラメーター	説明
名前	リファレンス・セット名の最大長は 255 文字です。

表 30. リファレンス・セットのパラメーター (続き)

パラメーター	説明
タイプ	リファレンス・エレメントのデータ・タイプを選択します。リファレンス・セットの作成後に「タイプ」パラメーターを編集することはできません。 「**IP**」タイプには、IPv4 のアドレスが格納されます。「英数字 **(**大**/**小文字は無視**)**」では、英数字の値が自動的に小文字に変更されます。 難読化されたイベント・プロパティーおよびフロー・プロパティーをリファレンス・データと比較するには、英数字のリファレンス・セットを使用する必要があります。
エレメントの存続時間	QRadar によってリファレンス・セットからエレメントが自動的に削除されるタイミングを指定します。デフォルトの設定は、「永久に存続」です。 時間を指定する場合は、存続時間間隔が、データが最初に確認された時間と最後に確認された時間のどちらに基づくのかを指定します。 リファレンス・セットのエレメントの有効期限が切れると、「リファレンス・データの期限切れ **(Reference Data Expiry)**」イベントがトリガーされます。このイベントには、リファレンス・セット名とエレメント値が含まれています。

b. 「作成」をクリックします。

3. 既存のリファレンス・セットを処理するには、「編集」または「削除」をクリックします。

   ヒント**:** 複数のリファレンス・セットを削除するには、「クイック検索」テキスト・ボックスを使用して、削除対象のリファレンス・セットを検索し、「リスト内容の削除」をクリックします。

関連タスク:

『リファレンス・セットの内容の表示』
リファレンス・セットのデータ・エレメントに関する情報 (ドメイン割り当て、データの有効期限、エレメントがネットワークで最後に確認された日時など) を確認します。

185 ページの『期限切れユーザー・アカウントの追跡』
リファレンス・データ収集を使用して、IBM Security QRadar 環境の失効したデータ (期限切れユーザー・アカウントなど) を特定します。

リファレンス・セットの内容の表示

リファレンス・セットのデータ・エレメントに関する情報 (ドメイン割り当て、データの有効期限、エレメントがネットワークで最後に確認された日時など) を確認します。

手順

1. 「管理」タブで、「リファレンス・セット管理」をクリックします。
2. リファレンス・セットを選択して、「内容の表示」をクリックします。
3. 「内容」タブをクリックして、各データ・エレメントに関する情報を表示します。

   ヒント: 検索フィールドを使用して、キーワードに一致するすべてのエレメントをフィルターに掛けます。「存続時間」列のデータの検索は実行できません。

   データ・エレメントに関する詳細の説明:

   以下の表に、リファレンス・セット内の各データ・エレメントについて表示される情報を示します。

表 *31.* リファレンス・セットのデータ・エレメントに関する情報

パラメーター	説明
ドメイン	ドメイン固有のリファレンス・データは、そのドメインへのアクセス権限を持つテナント・ユーザー、MSSP 管理者、およびテナントが割り当てられていないユーザーが参照できます。すべてのテナントのユーザーが、共有リファレンス・データを参照できます。
値	リファレンス・セットに格納されるデータ・エレメント。例えば、値には、ユーザー名、IP アドレスなどが表示されることがあります。
オリジン	データ・エレメントが手動で追加されたときはユーザー名が表示され、外部ファイルからインポートされてデータが追加されたときはファイル名が表示されます。ルールへの応答としてデータ・エレメントが追加されたときは、ルール名が表示されます。
存続時間 **(Time to Live)**	このエレメントがリファレンス・セットから削除されるまでの残り時間。
最終表示日 **(Date Last Seen)**	このエレメントがネットワーク上で最後に検出された日時。

4. 「リファレンス」タブをクリックして、ルール・テストまたはルール応答でリファレンス・セットを使用しているルールを表示します。

表 *32.* 「内容」タブのパラメーター

パラメーター	説明
ルール名	リファレンス・セットを使用するように構成されているルールの名前。
グループ	このルールが属するグループ。
カテゴリー	ルールがカスタム・ルールであるか、アノマリ検出ルールであるかを表示します。
タイプ	ルールのテスト対象のデータのタイプを示す、「イベント」、「フロー」、「共通」、または「オフェンス」を表示します。

表 32. 「内容」タブのパラメーター (続き)

パラメーター	説明
有効	カスタム・ルール・エンジンでルールを評価するには、そのルールが有効になっている必要があります。
応答 **(Response)**	このルール用に構成されている応答。
オリジン	「システム」は、デフォルトのルールを示します。 「変更済み」は、デフォルトのルールがカスタマイズされたことを示します。 「ユーザー」は、ユーザーが作成したルールを示します。

5. 関連付けられているルールを表示または編集するには、「リファレンス」リスト内のルールをダブルクリックし、ルール・ウィザードを実行します。

リファレンス・セットへのエレメントの追加

IBM Security QRadar でプロパティーをエレメント値と比較する場合、リファレンス・セットにエレメントを追加します。QRadar を使用して、リファレンス・セットに手動でエレメントを追加するか、または .csv ファイルからエレメントをインポートします。

始める前に

エレメントをインポートするには、.csv ファイルがローカルに保管されている必要があります。

このタスクについて

ドメイン固有のリファレンス・データは、そのドメインへのアクセス権限を持つテナント・ユーザー、MSSP 管理者、およびテナントが割り当てられていないユーザーが参照できます。すべてのテナントのユーザーが、共有リファレンス・データを参照できます。

リファレンス・データを特定のドメインに割り当てることができます。ドメイン固有のリファレンス・データは、そのドメインへのアクセス権限を持つテナント・ユーザー、MSSP 管理者、およびテナントが割り当てられていないユーザーが参照できます。すべてのテナントのユーザーが、共有リファレンス・データを参照できます。例えば、管理者でない MSSP ユーザーは、あるドメインに割り当てられているリファレンス・データを参照できます。

手順

1. 「管理」タブで、「リファレンス・セット管理」をクリックします。
2. エレメントを追加するリファレンス・セットを選択し、「内容の表示」をクリックします。
3. 「内容」タブをクリックします。
4. データ・エレメントを手動で追加するには、以下の手順を実行します。
   a. 「追加」をクリックし、パラメーターを構成します。

有効なポート値は 0 から 65535 までです。有効な IP アドレスは 0 から 255.255.255.255 までです。

注: リファレンス・セット・データを比較するイベント・プロパティーにデータ難読化技法を使用する場合、難読化されたデータ値を含む英数字のリファレンス・セットを使用する必要があります。

b. 「追加」をクリックします。

5. .csv ファイルからエレメントを追加するには、以下の手順を実行します。
   a. 「インポート」をクリックします。
   b. 「ファイルの選択」をクリックし、インポートする .csv ファイルを参照して選択します。

      .csv ファイルの形式は、1 行にすべてのアイテムがコンマ区切りでリストされているか、1 行に 1 アイテムずつリストされている必要があります。1 行に 1 アイテムずつリストされている場合は区切り文字は不要です。

   c. リファレンス・セット・データを追加する「ドメイン」を選択します。
   d. 「インポート」をクリックします。 インポートにより、テキスト・ファイルの内容がリファレンス・セットに追加されます。

リファレンス・セットからのエレメントのエクスポート

リファレンス・セットのエレメントの情報をレポートに含めるか、IBM Security QRadar を使用していないユーザーと共有するときは、.csv ファイルにリファレンス・セットのエレメントをエクスポートします。

手順

1. 「管理」タブで、「リファレンス・セット管理」をクリックします。
2. エクスポートするリファレンス・セットを選択し、「内容の表示」をクリックします。
3. 「内容」タブをクリックし、「エクスポート」をクリックします。
4. ファイルをすぐに開くか、ファイルを保存するかを選択し、「**OK**」をクリックします。

リファレンス・セットからのエレメントの削除

リファレンス・セットに誤ってエレメントが追加されたときや、他の IBM Security QRadar プロパティーとの比較にエレメントが必要なくなったときに、リファレンス・セットからエレメントを削除することが必要になる場合があります。例えば、アセット除外のブラックリストに誤って追加されたアセットを削除しなければならない場合があります。

手順

1. 「管理」タブで、「リファレンス・セット管理」をクリックします。
2. 削除するエレメントが含まれているリファレンス・セットを選択し、「内容の表示」を選択します。
3. 「内容」タブをクリックして、次のオプションのいずれかを選択します。

- 単一のエレメントを削除するには、リストでエレメントを選択し、「削除」をクリックします。
- 複数のエレメントを削除するには、検索ボックスを使用して削除対象のエレメントのみが表示されるようにリストをフィルターに掛け、「リスト内容の削除」をクリックします。

コマンド・ラインを使用したリファレンス・データ収集の作成

IBM Security QRadar で管理できないリファレンス・データ収集 (リファレンス・マップ、セットのマップ、マップのマップ、テーブルなど) の管理には、コマンド・ラインを使用します。QRadar を使用してリファレンス・セットを管理する方が簡単ですが、管理タスクをスケジュールするときには、コマンド・ラインを使用します。

このタスクについて

`ReferenceSetUtil.sh` スクリプトを使用してリファレンス・セットを管理します。`ReferenceDataUtil.sh` スクリプトを使用して、他のすべてのタイプのリファレンス・データ収集を管理します。

外部ファイルを使用してリファレンス・データ収集にデータを取り込む場合、ファイル内の最初の非コメント行は、リファレンス・データ収集の列名を表しています。それ以降の各行は、収集に追加されるデータ・レコードです。リファレンス収集の値のデータ・タイプは収集の作成時に指定されますが、各キーは英数字ストリングです。

以下の表に、リファレンス・マップへのデータの取り込みに使用される外部ファイル内のデータ・フォーマットの例を示します。

表 33. リファレンス・データ収集へのデータの取り込みに使用される外部ファイルのデータのフォーマット

リファレンス収集のタイプ	データ形式の設定例

リファレンス・マップ	`key1,data`
	`key1,value1`
	`key2,value2`

セットのリファレンス・マップ	`key1,data`
	`key1,value1`
	`key1,value2`

マップのリファレンス・マップ	`key1,key2,data`
	`map1,key1,value1`
	`map1,key2,value2`

QRadar RESTful API 内の `/reference_data` エンドポイントを使用して、リファレンス・データ収集を作成することもできます。

手順

1. SSH を使用して、root ユーザーとして IBM Security QRadar にログインします。
2. /opt/qradar/bin ディレクトリーに移動します。
3. リファレンス・データ収集を作成するための、以下のコマンドを入力します。

```
./ReferenceDataUtil.sh create name
[SET | MAP | MAPOFSETS | MAPOFMAPS | REFTABLE]
[ALN | NUM | IP | PORT | ALNIC | DATE]
[-timeoutType=[FIRST_SEEN | LAST_SEEN]] [-timeToLive=]
```

4. 外部ファイルからマップにデータを取り込むために、以下のコマンドを入力します。

```
./ReferenceDataUtil.sh load name filename
 [-encoding=...] [-sdf=" ... "]
```

例

コマンド・ラインを使用してさまざまなタイプのリファレンス・データ収集を作成する方法の例を次に示します。

- 英数字のマップを作成する方法:

```
./ReferenceDataUtil.sh create testALN MAP ALN
```

- 最後に確認されてから 3 時間後にエージアウトするポート値を含むセットのマップを作成する方法:

```
./ReferenceDataUtil.sh create testPORT MAPOFSETS PORT
-timeoutType=LAST_SEEN -timeToLive='3 hours'
```

- 最初に確認されてから 3 時間 15 分後にエージアウトする数値を含むマップのマップを作成する方法:

```
./ReferenceDataUtil.sh create testNUM MAPOFMAPS
NUM -timeoutType=FIRST_SEEN -timeToLive='3 hours 15 minutes'
```

- デフォルトのフォーマットが英数字であるリファレンス・テーブルを作成する方法:

```
./ReferenceDataUtil.sh create testTable REFTABLE
ALN -keyType=ipKey:IP,portKey:PORT,numKey:NUM,dateKey:DATE
```

次のタスク

QRadar にログインして、リファレンス・データ収集にデータを追加するルールを作成します。リファレンス・データ収集にあるエレメントからアクティビティーを検出するルール・テストを作成することもできます。

関連概念:

171 ページの『リファレンス・セット概要』

IBM Security QRadar のリファレンス・セットを使用して、単純なリスト形式でデータを保管します。

リファレンス・データ・ユーティリティーのコマンド・リファレンス

コマンド・ラインで ReferenceSetUtil.sh ユーティリティーおよび ReferenceDataUtil.sh ユーティリティーを使用して、リファレンス・データ収集を管理することができます。以下のコマンドのリストは、両方のスクリプトで使用することができます。

Create

リファレンス・データ収集を作成します。

name
リファレンス・データ収集の名前。

[SET | MAP | MAPOFSETS | MAPOFMAPS | REFTABLE]
リファレンス・データ収集のタイプ。ReferenceSetUtil.sh スクリプトは、リファレンス・セットの作成のみを行います。

[ALN | ALNIC | NUM | IP | PORT | DATE]
リファレンス・セット内のデータのタイプ。

- **ALN** は、英数字の値を指定します。このデータ・タイプは、IPv4 アドレスと IPv6 アドレスをサポートします。
- **ALNIC**は、英数字の値を指定しますが、ルール・テストでは大/小文字が無視されます。このデータ・タイプは、IPv4 アドレスと IPv6 アドレスをサポートします。
- **NUM** は、数値を指定します。
- **IP** は、IP アドレスを指定します。このデータ・タイプは、IPv4 アドレスだけをサポートします。
- **PORT** は、ポート・アドレスを指定します。
- **DATE** は、日付値を指定します。

[-timeoutType=[FIRST_SEEN | LAST_SEEN]]
リファレンス・データ収集内でのデータ・エレメントの存続時間を、データ・エレメントを最初に表示したときから計算するのか、最後に表示したときから計算するのかを指定します。

[-TimeToLive='']
リファレンス・データ収集内でのデータ・エレメントの存続時間。

[-keyType=name:elementType,name:elementType,...]
ELEMENTTYPE のペアに対するキー名から構成される必須の **REFTABLE** パラメーター。

[-key1Label='']
key1 またはプライマリー・キーのオプション・ラベル。キーは、あるタイプの情報 (例えば、IP アドレスなど) です。

[-valueLabel='']
コレクションの値に対するオプション・ラベル。

Update

リファレンス・データ収集を更新します。

name
リファレンス・データ収集の名前。

[-timeoutType=[FIRST_SEEN | LAST_SEEN]]
リファレンス・データ収集内でのデータ・エレメントの存続時間を、データ・エレメントを最初に表示したときから計算するのか、最後に表示したときから計算するのかを指定します。

[-timeToLive='']
リファレンス・データ収集内でのデータ・エレメントの存続時間。

[-keyType=name:elementType,name:elementType,...]
elementType のペアに対するキー名から構成される必須の **REFTABLE** パラメーター。

[-key1Label='']
key1 に対するオプション・ラベル。

[-valueLabel='']
コレクションの値に対するオプション・ラベル。

Add

データ・エレメントをリファレンス・データ収集に追加します。

name
リファレンス・データ収集の名前。

<value> <key1> [key2]
追加したいキー値のペア。キーは英数字ストリングです。

- MAP と MAPOFSETS には、キー 1 が必要です。
- MAPOFMAPS と REFTABLE には、キー 1 と、第 2 レベルのキー 2 が必要です。

[-sdf=" ... "]
日付データの解析に使用される単純な日付形式のストリング。

削除

リファレンス・データ収集からエレメントを削除します。

name
リファレンス・データ収集の名前。

<value> <key1> [key2]
削除したいキー値のペア。キーは英数字ストリングです。

- MAP と MAPOFSETS には、キー 1 が必要です。
- MAPOFMAPS と REFTABLE には、キー 1 と、第 2 レベルのキー 2 が必要です。

[-sdf=" ... "]
日付データの解析に使用される単純な日付形式のストリング。

Remove

リファレンス・データ収集を除去します。

name
リファレンス・データ収集の名前。

Purge
リファレンス・データ収集からすべてのエレメントをパージします。

name
リファレンス・データ収集の名前。

List
リファレンス・データ収集内のエレメントをリストします。

name
リファレンス・データ収集の名前。

[displayContents]
指定されたリファレンス・データ収集内のすべてのエレメントをリストします。

Listall
すべてのリファレンス・データ収集内のすべてのエレメントをリストします。

[displayContents]
すべてのリファレンス・データ収集内のすべてのエレメントをリストします。

Load
外部の .csv ファイルのデータをリファレンス・データ収集に取り込みます。

name
リファレンス・データ収集の名前。

filename
ロードする完全修飾ファイル名。ファイル内の各行は、リファレンス・データ収集に追加されるレコードを表しています。

[-encoding=...]
ファイルの読み取りに使用されるエンコード。

[-sdf=" ... "]
日付データの解析に使用される単純な日付形式のストリング。

API を使用したリファレンス・データ収集の作成
アプリケーション・プログラム・インターフェース (API) を使用して、IBM Security QRadar のリファレンス・データ収集を管理できます。

手順
1. Web ブラウザーを使用して https://<*Console IP*>/api_doc にアクセスし、管理者としてログインします。
2. IBM Security QRadar API の最新の反復を選択します。
3. /reference_data ディレクトリーを選択します。
4. 新しいリファレンス・セットを作成するには、次の手順に従います。
   a. /sets を選択します。

b. 「**POST**」をクリックし、「値」フィールドに関連情報を入力します。

リファレンス・セットを作成するためのパラメーターに関する詳細:

リファレンス・セットの作成に必要なパラメーターに関する情報を次の表に示します。

表 *34.* パラメーター - リファレンス・セット

パラメーター	タイプ	値	データ・タイプ	**MIME** タイプ	サンプル
element_type	query	(必須)	String	text/plain	String <ALN, NUM, IP, PORT, ALNIC, DATE> のいずれか
name	query	(必須)	String	text/plain	String
fields	query	(オプション)	String	text/plain	field_one (field_two, field_three), field_four
time_to_live	query	(オプション)	String	text/plain	String
timeout_type	query	(オプション)	String	text/plain	String <UNKNOWN, FIRST_SEEN, LAST_SEEN> のいずれか

c. 「試用」をクリックして、リファレンス・データ収集の作成を終了し、結果を確認します。

5. 新しいリファレンス・マップを作成するには、次の手順に従います。

a. `/maps` をクリックします。

b. 「**POST**」をクリックし、「値」フィールドに関連情報を入力します。

リファレンス・マップを作成するためのパラメーターに関する詳細:

リファレンス・マップの作成に必要なパラメーターに関する情報を次の表に示します。

表 *35.* パラメーター - リファレンス・マップ

パラメーター	タイプ	値	データ・タイプ	**MIME** タイプ	サンプル
element_type	query	(必須)	String	text/plain	String <ALN, NUM, IP, PORT, ALNIC, DATE> のいずれか
name	query	(必須)	String	text/plain	String

表 35. パラメーター - リファレンス・マップ (続き)

パラメーター	タイプ	値	データ・タイプ	MIME タイプ	サンプル
fields	query	(オプション)	String	text/plain	field_one (field_two, field_three), field_four
key_label	query	(オプション)	String	text/plain	String
time_to_live	query	(オプション)	String	text/plain	String
timeout_type	query	(オプション)	String	text/plain	String <UNKNOWN, FIRST_SEEN, LAST_SEEN> のいずれか
value_label	query	(オプション)	String	text/plain	String

c. 「試用」をクリックして、リファレンス・データ収集の作成を終了し、結果を確認します。

6. 新しいセットのリファレンス・マップを作成するには、次の手順に従います。
   a. `/map_of_sets` を選択します。
   b. 「**POST**」をクリックし、「値」フィールドに関連情報を入力します。

      セットのリファレンス・マップを作成するためのパラメーターに関する詳細:

      セットのリファレンス・マップの作成に必要なパラメーターに関する情報を次の表に示します。

表 36. パラメーター - セットのリファレンス・マップ

パラメーター	タイプ	値	データ・タイプ	MIME タイプ	サンプル
element_type	query	(必須)	String	text/plain	String <ALN, NUM, IP, PORT, ALNIC, DATE> のいずれか
name	query	(必須)	String	text/plain	String
fields	query	(オプション)	String	text/plain	field_one (field_two, field_three), field_four
key_label	query	(オプション)	String	text/plain	String
time_to_live	query	(オプション)	String	text/plain	String

表 36. パラメーター - セットのリファレンス・マップ (続き)

パラメーター	タイプ	値	データ・タイプ	MIME タイプ	サンプル
timeout_type	query	(オプション)	String	text/plain	String <UNKNOWN, FIRST_SEEN, LAST_SEEN> のいずれか
value_label	query	(オプション)	String	text/plain	String

c. 「試用」をクリックして、リファレンス・データ収集の作成を終了し、結果を確認します。

7. 新しいセットのリファレンス・テーブルまたはマップのマップを作成するには、次の手順に従います。

a. `/tables` をクリックします。

b. 「**POST**」をクリックし、「値」フィールドに関連情報を入力します。

リファレンス・テーブルまたはマップのマップを作成するためのパラメーターに関する詳細:

リファレンス・テーブルまたはマップのマップの作成に必要なパラメーターに関する情報を次の表に示します。

表 37. パラメーター - リファレンス・テーブル

パラメーター	タイプ	値	データ・タイプ	MIME タイプ	サンプル
element_type	query	(必須)	String	text/plain	String <ALN, NUM, IP, PORT, ALNIC, DATE> のいずれか
name	query	(必須)	String	text/plain	String
fields	query	(オプション)	String	text/plain	field_one (field_two, field_three), field_four
key_name_types	query	(オプション)	Array	application/json	[{ "element_type": "String <ALN, NUM, IP, PORT, ALNIC, DATE> のいずれか", "key_name": "String" }]
outer_key_label	query	(オプション)	String	text/plain	String
time_to_live	query	(オプション)	String	text/plain	String

表 37. パラメーター - リファレンス・テーブル (続き)

パラメーター	タイプ	値	データ・タイプ	MIME タイプ	サンプル
timeout_type	query	(オプション)	String	text/plain	String <UNKNOWN, FIRST_SEEN, LAST_SEEN> のいずれか

c. 「試用」をクリックして、リファレンス・データ収集の作成を終了し、結果を確認します。

関連概念:

171 ページの『リファレンス・セット概要』

IBM Security QRadar のリファレンス・セットを使用して、単純なリスト形式でデータを保管します。

リファレンス・データ収集の使用例

これらの例では、リファレンス・データ収集を使用して、QRadar の検索、フィルター、ルール・テスト条件、およびルール応答で使用するデータを追跡および保管する方法を示します。

期限切れユーザー・アカウントの追跡

リファレンス・データ収集を使用して、IBM Security QRadar 環境の失効したデータ (期限切れユーザー・アカウントなど) を特定します。

このタスクについて

デフォルトでは、リファレンス・データは、削除されるまで QRadar に残ります。ただし、リファレンス・データ収集を作成するときに、指定の期間経過後にデータを削除するように QRadar を構成することができます。

データ・エレメントが期限切れになると、QRadar は自動的にリファレンス・データ収集から値を削除し、期限切れを追跡するためのイベントをトリガーします。

手順

1. ユーザーが最後にログインしてからの経過時間を追跡するためのリファレンス・セットを作成します。
   a. 「エレメントの存続時間」を設定します。使用されていないユーザー・アカウントは、この期間が過ぎると、期限切れと見なされます。
   b. 「最後の確認以降」ボタンを選択します。
2. **username** などのログイン・データをリファレンス・セットに追加するためのカスタム・イベント・ルールを作成します。

   注**:** QRadar は、各データ・エレメントの「最終表示日」を追跡します。存続時間内に特定のユーザーについてのデータが追加されない場合、リファレンス・セット・エレメントの期限が切れ、「リファレンス・データの期限切れ

(Reference Data Expiry)」イベントが起動されます。このイベントには、リファレンス・セット名と期限切れユーザー名が含まれています。

3. 「ログ・アクティビティー」タブを使用して、「リファレンス・データの期限切れ **(Reference Data Expiry)**」イベントを追跡します。

次のタスク

検索、フィルター、ルール・テスト条件、およびルール応答で、リファレンス・セット・データを使用します。

関連タスク:

172 ページの『リファレンス・セットの追加、編集、および削除』
リファレンス・セットは、IP アドレスやユーザー名などのプロパティー値をリストに照らして比較するために使用します。リファレンス・セットをルールと共に使用して、ウォッチ・リストを維持できます。例えば、禁止されている Web サイトにアクセスする従業員を検出して、その従業員の IP アドレスをリファレンス・セットに追加するためのルールを作成できます。

外部ソースからの動的データの統合

規模の大きな企業組織では、リファレンス・データ収集を使用して、組織の IT アセットに関する情報を、IBM Security QRadar デプロイメントを管理するセキュリティー・チームと共用することができます。

例えば、情報技術 (IT) チームは、すべてのネットワーク・アセットに関する情報が含まれているアセット管理データベースを管理しています。一部の情報 (Web サーバーの IP アドレスなど) は、頻繁に変わります。

週に 1 回、IT チームはネットワークにデプロイされているすべての Web サーバーの IP アドレスのリストをエクスポートし、そのリストをセキュリティー・チームに提供します。セキュリティー・チームはこのリストをリファレンス・セットにインポートします。これをルール、検索、およびレポートで使用して、QRadar によって処理されるイベントおよびフローに詳細なコンテキストを提供できます。

第 9 章 ユーザー情報ソースの構成

Identity and Access Management エンドポイントからユーザー情報とグループ情報を収集するために、IBM Security QRadar システムを構成します。

QRadar は、エンドポイントから収集された情報を使用して、ネットワーク上で発生したトラフィックとイベントに関連するユーザー情報を拡張します。

関連概念:

5 ページの『IBM Security QRadar 製品の機能』
IBM Security QRadar 製品資料では、オフェンス、フロー、アセット、ヒストリカル相関などの機能について説明していますが、すべての QRadar 製品でこれらの機能を利用できるわけではありません。使用する製品によっては、説明されている一部の機能をデプロイメントで使用できない場合があります。各製品の機能を確認して、必要な情報を入手してください。

ユーザー情報ソースの概要

ユーザー情報ソースを構成して、Identity and Access Management エンドポイントからユーザー情報を収集することができます。

Identity and Access Management エンドポイントは、電子ユーザー・アイデンティティー、グループ・メンバーシップ、アクセス権限を収集して管理する製品です。これらのエンドポイントはユーザー情報ソースと呼ばれます。

以下のユーティリティーを使用して、ユーザー情報ソースの構成と管理を行います。

- **Tivoli Directory Integrator** - 非 IBM Security QRadar ホスト上で Tivoli® Directory Integrator のインストールと構成を行う必要があります。
- **UISConfigUtil.sh** - このユーティリティーを使用して、ユーザー情報ソースの作成、取得、更新、削除を行います。ユーザー情報ソースを使用して、Tivoli Directory Integrator サーバーを使用する IBM Security QRadar SIEM を統合することができます。
- **GetUserInfo.sh** - このユーティリティーを使用して、ユーザー情報ソースからユーザー情報を収集し、その情報をリファレンス・データ収集に格納します。このユーティリティーを使用して、オンデマンドでユーザー情報を収集することも、スケジュールに従ってユーザー情報を収集することもできます。

ユーザー情報ソース

ユーザー情報ソースは、エンドポイントとの通信を有効にしてユーザー情報とグループ情報を取得するための構成可能なコンポーネントです。

IBM Security QRadar システムは、以下のユーザー情報ソースをサポートしています。

表 38. サポートされる情報ソース

情報ソース	収集される情報
Microsoft Windows Active Directory (AD) バージョン 2008 - Microsoft Windows AD は、Windows ネットワークを使用するすべてのユーザーとコンピューターの認証と許可を行うディレクトリー・サービスです。	• full_name • user_name • user_principal_name • family_name • given_name • account_is_disabled • account_is_locked • password_is_expired • password_can_not_be_changed • no_password_expired • password_does_not_expire
IBM Security Access Manager (ISAM) バージョン 7.0 - ISAM は、企業 Web、クライアント/サーバー、既存のアプリケーション用の認証および許可ソリューションです。詳しくは、IBM Security Access Manager (ISAM) の資料を参照してください。	• name_in_rgy • first-name • last-name • account_valid • password_valid
IBM Security Identity Manager (ISIM) バージョン 6.0 - ISIM は、ポリシー・ベースのプロビジョニング・ソリューションをデプロイするためのソフトウェアとサービスを提供します。この製品は、閉鎖された企業環境内であるかどうか、仮想企業や大規模企業全体にわたるかどうかにかかわらず、従業員、請負業者、IBM ビジネス・パートナーに対して必要なアプリケーションへのアクセス権限を付与するプロセスを自動化します。詳しくは、IBM Security Integration Manager (ISIM) の資料を参照してください。	• 氏名 • DN

ユーザー情報用のリファレンス・データ収集

このトピックでは、ユーザー情報ソースから収集されたデータをリファレンス・データ収集に格納する方法について説明します。

IBM Security QRadar SIEM は、ユーザー情報ソースから情報を収集する際に、その情報を格納するためのリファレンス・データ収集を自動的に作成します。リファレンス・データ収集の名前は、ユーザー情報ソースのグループ名から取得されます。例えば、Microsoft Windows AD から収集されたリファレンス・データ収集には、「Domain Admins」などの名前が付けられます。

リファレンス・データ収集のタイプは、マップのリファレンス・マップです。マップのリファレンス・マップでは、データは、あるキーを別のキーにマップするレコードに格納されます。次に、このデータが単一の値にマップされます。

例えば、以下のようにします。

- `#`
- `# Domain Admins`
- `# key1,key2,data`
- `smith_j,Full Name,John Smith`
- `smith_j,account_is_disabled,0`
- `smith_j,account_is_locked,0`
- `smith_j,account_is_locked,1`
- `smith_j,password_does_not_expire,1`

リファレンス・データ収集について詳しくは、「*Reference Data Collections Technical Note*」を参照してください。

統合ワークフローの例

ユーザー情報とグループ情報が収集され、リファレンス・データ収集に格納されると、さまざまな方法でそれらのデータを IBM Security QRadar SIEM で使用することができます。

会社のセキュリティー・ポリシーに対するユーザーの順守を示す有効なレポートとアラートを作成することができます。

ここでは、以下の例について考えてみます。

特権 ISIM ユーザーが実行するアクティビティーがセキュリティー・ポリシーに準拠するようにするには、以下のタスクを実行します。

各 ISIM サーバーの監査データを収集して解析するためのログ・ソース (ログの収集元) を作成します。ログ・ソースを作成する方法について詳しくは、「*Managing Log Sources Guide*」を参照してください。

1. ISIM サーバー用のユーザー情報ソースを作成して、ISIM 管理者ユーザー・グループ情報を収集します。このステップにより、「ISIM 管理者」というリファレンス・データ収集が作成されます。 193 ページの『ユーザー情報ソースの作成』を参照してください。
2. 送信元 IP アドレスが ISIM サーバーで、ユーザー名が ISIM 管理者リファレンス・データ収集にリストされているイベントをテストするビルディング・ブロックを構成します。ビルディング・ブロックについて詳しくは、「ユーザーズ・ガイド」を参照してください。
3. カスタムのビルディング・ブロックをフィルターとして使用するイベント検索を作成します。イベント検索について詳しくは、「*IBM Security QRadar* ユーザー・ガイド」を参照してください。
4. カスタム・イベントを使用するカスタム・レポートを作成し、特権 ISIM ユーザーの監査アクティビティーに関する日次レポートを生成します。生成されたレポートには、セキュリティー・ポリシーに違反している ISIM 管理者アクティビティーかないかどうかが示されます。レポートについて詳しくは、「*IBM Security QRadar* ユーザー・ガイド」を参照してください。

注: アプリケーション・セキュリティー・ログを収集する場合は、デバイス・サポート・モジュール (DSM) を作成する必要があります。詳しくは、「*IBM Security QRadar DSM Configuration Guide*」を参照してください。

ユーザー情報ソースの構成と管理タスクの概要

ユーザー情報ソースを初めて統合する場合は、以下のタスクを実行する必要があります。

1. Tivoli Directory Integrator サーバーを構成します。『Tivoli Directory Integrator サーバーの構成』を参照してください。
2. ユーザー情報ソースを作成して管理します。 193 ページの『ユーザー情報ソースの作成と管理』を参照してください。
3. ユーザー情報を収集します。 196 ページの『ユーザー情報の収集』を参照してください。

Tivoli Directory Integrator サーバーの構成

IBM Security QRadar とユーザー情報ソースを統合するには、QRadar 以外のホストに Tivoli Directory Integrator をインストールして構成する必要があります。

このタスクについて

QRadar システムで構成を行う必要はありませんが、コンソールにアクセスして `QRadarIAM_TDI.zip` ファイルを取得する必要があります。次に、別のホストで Tivoli Directory Integrator サーバーのインストールと構成を行います。自己署名証明書を作成し、インポートします。

Tivoli Directory Integrator サーバー上で `QRadarIAM_TDI.zip` ファイルを抽出すると、TDI ディレクトリーが自動的に作成されます。TDI ディレクトリーには、以下のファイルが格納されています。

- `QradarIAM.sh`: Linux 用の TDI 起動スクリプト
- `QradarIAM.bat`: Microsoft Windows 用の TDI 起動スクリプト。
- `QradarIAM.xml`: TDI xml スクリプト。`QradarIAM.properties` ファイルと同じ場所に格納する必要があります。
- `QradarIAM.properties`: TDI xml スクリプト用のプロパティー・ファイル。

Tivoli Directory Integrator をインストールする場合は、Solutions ディレクトリーの名前を構成する必要があります。このタスクでは、Solutions ディレクトリーにアクセスする必要があります。そのため、このタスクのステップの *<solution_directory>* は、このディレクトリーの名前を表しています。

以下のパラメーターを使用して、証明書の作成とインポートを行います。

表 *39.* 証明書の構成パラメーター

パラメーター	説明
<server_ip_address>	Tivoli Directory Integrator サーバーの IP アドレスを定義します。
<days_valid>	証明書の有効日数を定義します。

表 39. 証明書の構成パラメーター (続き)

パラメーター	説明
<keystore_file>	鍵ストア・ファイルの名前を定義します。
-storepass *<password>*	鍵ストアのパスワードを定義します。
- keypass *<password>*	秘密鍵と公開鍵のペアのパスワードを定義します。
<alias>	エクスポートされた証明書の別名を定義します。
<certificate_file>	証明書のファイル名を定義します。

手順

1. QRadar 以外のホストに Tivoli Directory Integrator をインストールします。Tivoli Directory Integrator のインストール方法と構成方法については、Tivoli Directory Integrator (TDI) の資料を参照してください。
2. SSH を使用して、root ユーザーとして IBM Security QRadar コンソールにログインします。
   a. ユーザー名: `root`
   b. パスワード: *<password>*
3. `QRadarIAM_TDI.zip` ファイルを Tivoli Directory Integrator サーバーにコピーします。
4. Tivoli Directory Integrator サーバーで、`QRadarIAM_TDI.zip` ファイルを Solutions ディレクトリーに抽出します。
5. QRadar と統合するように Tivoli Directory Integrator サーバーを構成します。
   a. Tivoli Directory Integrator の *<solution_directory>*`/solution.properties` ファイルを開きます。
   b. `com.ibm.di.server.autoload` プロパティーのコメントを外します。このプロパティーのコメントが既に外れている場合は、プロパティーの値をメモしておきます。
   c. 次のオプションのいずれかを選択してください。
      - 各ディレクトリーを `autoload.tdi` ディレクトリーに変更する (このディレクトリーには、`com.ibm.di.server.autoload` プロパティーがデフォルトで格納されています)。
      - *<solution_directory>* 内に、`com.ibm.di.server.autoload` プロパティーを格納するための `autoload.tdi` ディレクトリーを作成する。
   d. `TDI/QRadarIAM.xml` ファイルと `TDI/QRadarIAM.property` ファイルを、Tivoli Directory Integrator ディレクトリーから *<solution_directory>*`/autoload.tdi` ディレクトリーまたは前のステップで作成したディレクトリーに移動します。
   e. `QradarIAM.bat` および `QradarIAM.sh` スクリプトを、Tivoli Directory Integrator ディレクトリーから Tivoli Directory Integrator を開始する場所に移動します。
6. 自己署名証明書を作成して、Tivoli Directory Integrator トラストストアにインポートします。

a. 鍵ストアと、秘密鍵/公開鍵のペアを生成するには、以下のコマンドを入力します。
   - keytool -genkey -dname cn=<*server_ip_address*> -validity <*days_valid*> -keystore <*keystore_file*> -storepass <*password*> -keypass <*password*>
   - 以下に例を示します。keytool -genkey -dname cn=192.168.1.1 -validity 365 -keystore server.jks -storepass secret -keypass secret

b. 証明書を鍵ストアからエクスポートするには、以下のコマンドを入力します。
   - keytool -export -alias <*alias*> -file <*certificate_file*> -keystore <*keystore_file*> - storepass <*password*>
   - 以下に例を示します。keytool -export -alias mykey -file server.cert -keystore server.jks -storepass secret

c. プライマリー証明書を自己署名 CA 証明書として鍵ストアにインポートするには、以下のコマンドを入力します。
   - keytool -import -trustcacerts -file <*certificate_file*> -keystore <*keystore_file*> -storepass <*password*> -alias <*alias*>
   - 以下に例を示します。keytool -import -trustcacerts -file server.cert -keystore server.jks -storepass secret -alias mytrustedkey

d. QRadar コンソール で、証明書ファイルを /opt/qradar/conf/trusted_certificates にコピーします。

7. CA 証明書を Tivoli Directory Integrator トラストストアにインポートします。
   a. CA 証明書を自己署名 CA 証明書として鍵ストアにインポートするには、以下のコマンドを入力します。
      - keytool -import -trustcacerts -file <*certificate_file*> -keystore <*keystore_file*> -storepass <*password*> -alias <*alias*>
      - 以下に例を示します。keytool -import -trustcacerts -file server.cert -keystore server.jks -storepass secret -alias mytrustedkey

   b. QRadar コンソール で、CA 証明書ファイルを /opt/qradar/conf/trusted_certificates にコピーします。

8. <solution_directory>/solution.properties ファイルを編集し、以下のプロパティーのコメントを外して構成します。
   - javax.net.ssl.trustStore=<*keystore_file*>
   - {protect}-javax.net.ssl.trustStorePassword=<*password*>
   - javax.net.ssl.keyStore=<*keystore_file*>
   - {protect}-javax.net.ssl.keyStorePassword=<*password*>

注: 変更されていないデフォルトのパスワードが、以下の形式で表示される場合があります。{encr}EyHbak。プレーン・テキストでパスワードを入力してください。Tivoli Directory Integrator を初めて始動すると、パスワードが暗号化されます。

9. Tivoli Directory Integrator を始動します。

ユーザー情報ソースの作成と管理

UISConfigUtil ユーティリティーを使用して、ユーザー情報ソースの作成、取得、更新、削除を行います。

ユーザー情報ソースの作成

UISConfigUtil ユーティリティーを使用して、ユーザー情報ソースを作成します。

始める前に

ユーザー情報ソースを作成する前に、Tivoli Directory Integrator サーバーをインストールして構成する必要があります。詳しくは、 190 ページの『Tivoli Directory Integrator サーバーの構成』を参照してください。

このタスクについて

ユーザー情報ソースを作成する場合は、ユーザー情報ソースを構成するために必要なプロパティー値を特定する必要があります。以下の表で、サポートされるプロパティー値について説明します。

表 *40.* サポートされるユーザー・インターフェースのプロパティー値

プロパティー	説明
tdiserver	Tivoli Directory Integrator サーバーのホスト名を定義します。
tdiport	Tivoli Directory Integrator サーバーの HTTP コネクターの listen ポートを定義します。
hostname	ユーザー情報ソース・ホストのホスト名を定義します。
port	ユーザー情報ホストの Identity and Access Management レジストリーの listen ポートを定義します。
username	IBM Security QRadar SIEM および が Identity and Access Management レジストリーへの認証で使用するユーザー名を定義します。
password	Identity and Access Management レジストリーへの認証に必要なパスワードを定義します。
searchbase	基本 DN を定義します。 **注:** すべてのグループで参照されるすべてのユーザーは、searchbase から行う検索で見つからなければなりません。

表 40. サポートされるユーザー・インターフェースのプロパティー値 (続き)

プロパティー	説明
search filter	Identity and Access Management レジストリーから取得されたグループをフィルタリングするために必要な検索フィルターを定義します。

手順

1. SSH を使用して、root ユーザーとして IBM Security QRadar コンソールにログインします。
   a. ユーザー名: root
   b. パスワード: <password>
2. ユーザー情報ソースを追加するために、次のコマンドを入力します。
   UISConfigUtil.sh add <name> -t <AD|ISAM|ISIM|ISFIM> [-d description] [-p prop1=value1,prop2=value2...,propn=valuen]

   各項目の意味は次のとおりです。
   - <name> は、追加するユーザー情報ソースの名前です。
   - <AD|ISAM|ISIM|ISFIM> は、ユーザー情報ソースのタイプです。
   - [-d description] は、ユーザー情報ソースの説明です。このパラメーターはオプションです。
   - [-p prop1=value1,prop2=value2,...,propn=valuen] は、ユーザー情報ソースに必要なプロパティー値です。サポートされるパラメーターについて詳しくは、 193 ページの『ユーザー情報ソースの作成』を参照してください。

   例えば、以下のようにします。
   - /UISConfigUtil.sh add "UIS_ISIM" -t ISIM -d "UIS for ISIM" -p "tdiserver=nc9053113023.tivlab.austin.ibm.com,tdiport=8080, hostname=vmibm7094.ottawa.ibm.com,port=389, username=cn=root,password=password,¥"searchbase=ou=org,DC=COM¥",¥ "searchfilter=(|(objectClass=erPersonItem)(objectClass=erBPPersonItem) (objectClass=erSystemUser))¥""

ユーザー情報ソースの取得

UISConfigUtil ユーティリティーを使用して、ユーザー情報ソースを取得します。

手順

1. SSH を使用して、root ユーザーとして IBM Security QRadar コンソールにログインします。
   a. ユーザー名: root
   b. パスワード: <password>
2. 次のオプションのいずれかを選択してください。
   a. 以下のコマンドを入力して、すべてのユーザー情報ソースを取得する。
      UISConfigUtil.sh get <name>
   b. 以下のコマンドを入力して、特定のユーザー情報ソースを取得する。
      UISConfigUtil.sh get <name>

<name> は、取得するユーザー情報ソースの名前です。

例えば、以下のようにします。

```
[root@vmibm7089 bin]# .UISConfigUtil.sh get "UIS_AD"
```

ユーザー情報ソースの編集

UISConfigUtil ユーティリティーを使用して、ユーザー情報ソースを編集します。

手順

1. SSH を使用して、root ユーザーとして IBM Security QRadar コンソールにログインします。
   a. ユーザー名: root
   b. パスワード: <password>
2. ユーザー情報ソースを編集するための次のコマンドを入力します。
   ```
   UISConfigUtil.sh update <name> -t <AD|ISAM|ISIM|ISFIM> [-d description]
   [-p prop1=value1,prop2=value2,...,propn=valuen]
   ```

   各項目の意味は次のとおりです。

   - <name> は、編集するユーザー情報ソースの名前です。
   - <AD|ISAM|ISIM|ISFIM> は、ユーザー情報ソースのタイプです。このパラメーターを更新するには、新しい値を入力します。
   - [-d description] は、ユーザー情報ソースの説明です。このパラメーターはオプションです。このパラメーターを更新するには、新しい説明を入力します。
   - [-p prop1=value1,prop2=value2,...,propn=valuen] は、ユーザー情報ソースに必要なプロパティー値です。このパラメーターを更新するには、new properties を入力します。サポートされるパラメーターについて詳しくは、193 ページの『ユーザー情報ソースの作成』を参照してください。

   例えば、以下のようにします。

   ```
   ./UISConfigUtil.sh update "UIS_AD_update" -t AD -d "UIS for AD" -p
   "searchbase=DC=local"
   ```

ユーザー情報ソースの削除

ユーザー情報ソースを削除するには、UISConfigUtil ユーティリティーを使用します。

手順

1. SSH を使用して、root ユーザーとして IBM Security QRadar コンソールにログインします。
   a. ユーザー名: root
   b. パスワード: <password>
2. 以下のコマンドを入力して、ユーザー情報ソースを削除します。

   ```
   UISConfigUtil.sh delete <name>
   ```

<name> は、削除するユーザー情報ソースの名前です。

次のタスク

収集されたユーザー情報が、IBM Security QRadar データベースのリファレンス・データ収集に格納されます。リファレンス・データ収集が存在しない場合は、新しいリファレンス・データ収集が作成されます。このユーザー情報ソースのリファレンス・データ収集が既に作成されている場合は、リファレンス・マップから以前のデータがパージされ、新しいユーザー情報が格納されます。リファレンス・データ収集について詳しくは、リファレンス・データ収集を参照してください。

ユーザー情報の収集

GetUserInfo ユーティリティーを使用してユーザー情報ソースからユーザー情報を収集し、そのデータをリファレンス・データ収集に格納します。

このタスクについて

このタスクを実行して、オンデマンドでユーザー情報を収集します。自動ユーザー情報コレクションをスケジュールに従って作成する場合は、cron ジョブ項目を作成します。cron ジョブについて詳しくは、Linux の資料を参照してください。

手順

1. SSH を使用して、root ユーザーとして IBM Security QRadar コンソールにログインします。
   a. ユーザー名: root
   b. <password>
2. 以下のコマンドを入力して、オンデマンドでユーザー情報を収集します。

   ```
   GetUserInfo.sh <UISName>
   ```

   <UISName> は、情報の収集元となるユーザー情報ソースの名前です。

次のタスク

収集されたユーザー情報が、データベースのリファレンス・データ収集に格納されます。リファレンス・データ収集が存在しない場合は、新しいリファレンス・データ収集が作成されます。このユーザー情報ソースのリファレンス・データ収集が既に作成されている場合は、リファレンス・マップから以前のデータがパージされ、新しいユーザー情報が格納されます。リファレンス・データ収集について詳しくは、188 ページの『ユーザー情報用のリファレンス・データ収集』を参照してください。

第 10 章 IBM X-Force の統合

IBM X-Force のセキュリティーの専門家は、一連の国際データ・センターを使用して数万件のマルウェアのサンプルを収集し、さまざまな Web ページと URL の分析を行い、解析処理を実行して潜在的に悪意のある IP アドレスと URL を分類します。このデータを IBM Security QRadar に統合し、望ましくないアクティビティーによってネットワークの安定性が影響を受ける前に、ご使用の環境でそうしたアクティビティーを検出して修正することにより、組織が新たな脅威に対して前もって対策を講じることができます。

例えば、以下のタイプのインシデントを識別および優先順位付けすることができます。

- 動的 IP アドレス範囲に対する連続したログイン試行
- ビジネス・パートナー・ポータルへの匿名プロキシー接続
- 内部エンドポイントと既知のボットネット・コマンドやコントロールの間の接続
- エンドポイントと既知のマルウェア配布サイトの間の通信

関連概念:

5 ページの『IBM Security QRadar 製品の機能』

IBM Security QRadar 製品資料では、オフェンス、フロー、アセット、ヒストリカル相関などの機能について説明していますが、すべての QRadar 製品でこれらの機能を利用できるわけではありません。使用する製品によっては、説明されている一部の機能をデプロイメントで使用できない場合があります。各製品の機能を確認して、必要な情報を入手してください。

「インターネット脅威インフォメーション・センター」ダッシュボード・ウィジェット

「脅威およびセキュリティーのモニター」ダッシュボードの「インターネット脅威インフォメーション・センター」ウィジェットは、X-Force データを使用して、セキュリティー問題、毎日の脅威の評価、セキュリティー・ニュース、および脅威リポジトリーに関して最新の勧告を提供します。

ダッシュボード・ウィジェットは、組み込みの RSS フィードを使用して、X-Force データをダッシュボード・ウィジェットに表示します。X-Force 更新サーバー (www.iss.net) からデータを受信するには、QRadar コンソールがインターネットにアクセスできる必要があります。

ダッシュボードは、4 つの AlertCon 脅威レベル・イメージを使用して、現在の脅威レベルの視覚的な指標を提供します。

表 41. AlertCon 脅威レベル

レベル	タイプ	説明
1	通常の脅威	QRadar がインターネットに接続した後、数分から数時間、無保護のネットワークを危険にさらす通常のアクティビティー。
2	警戒度引き上げ	脆弱性の評価と是正処置が必要な、コンピューター・ネットワークに対する脆弱性またはオンライン脅威。
3	集中的攻撃	インターネット攻撃の標的となっていて、直ちに防御処置が必要な特定の弱点および脆弱性。
4	破壊的脅威	即時の集中的防御処置が求められる、ネットワーク内の重大なセキュリティー状況。この状態は、その発生が差し迫っている場合、または現在発生中の場合があります。

現在の脅威レベルについて詳しくは、「詳細」リンクをクリックして、IBM X-Force Exchange Web サイトの「現在の脅威アクティビティー (Current Threat Activity)」ページを開いてください。

現在の勧告のサマリーを表示するには、その勧告の横の矢印アイコンをクリックします。勧告の詳細をすべて確認するには、その勧告のリンクをクリックします。

IBM Security Threat Content アプリケーション

IBM Security App Exchange (https://exchange.xforce.ibmcloud.com/hub) にある IBM Security Threat Content アプリケーションには、X-Force フィード・データと組み合わせて使用することを意図したルール、ビルディング・ブロック、およびカスタム・プロパティーが含まれています。

X-Force データには、潜在的に悪意のある IP アドレスと URL のリストが、対応する脅威スコアとともに含まれています。X-Force ルールを使用して、そのアドレスを含むセキュリティー・イベントやネットワーク・アクティビティーに自動的にフラグを立て、インシデントの調査を開始する前にそれらの優先順位付けを行います。

X-Force ルールを使用して識別できるインシデントのタイプの例を次のリストに示します。

- ***[source IP|destinationIP|anyIP]*** が、次の ***[remote network locations]*** のいずれかの一部であるとき
- ***[this host property]*** が、**X-Force** によって信頼値 ***[equal to] [this amount]*** で ***[Anonymization Servers|Botnet C&C|DynamicIPs|Malware|ScanningIPs|Spam]*** というカテゴリーに分類されているとき
- ***[this URL property]*** が、**X-Force** によって ***[Gambling|Auctions|Job Search|Alcohol|Social Networking|Dating]*** というカテゴリーに分類されているとき

IBM Security Threat Content アプリケーションでの X-Force Threat Intelligence フィードの使用を有効にすると、QRadar は、1 日あたり約 30 MB の IP レピュテーション・データをダウンロードします。

IBM Security Threat Content アプリケーションのインストール

IBM Security Threat Content アプリケーションには、X-Force データとともに使用することに特化して設計されたルール、ビルディング・ブロック、カスタム・プロパティーなどの IBM Security QRadar のコンテンツが含まれています。この拡張コンテンツを使用すると、望ましくないアクティビティーによってネットワークの安定性が影響を受ける前に、ご使用の環境でそうしたアクティビティーを特定して修正することができます。

始める前に

IBM Security App Exchange (https://exchange.xforce.ibmcloud.com/hub) から IBM Security Threat Content アプリケーションをダウンロードします。

このタスクについて

QRadar のルール、オフェンス、およびイベントで X-Force データを使用するには、X-Force サーバーから QRadar アプライアンスにデータを自動的にロードするように IBM Security QRadar を構成する必要があります。

ローカルに X-Force データをロードするには、システム設定で X-Force Threat Intelligence フィードを有効にします。X-Force の開始時に新規情報が使用可能である場合は、IP アドレス・レピュテーションまたは URL データベースが更新されます。これらの更新は独自のデータベースにマージされ、その内容は QRadar コンソール からデプロイメント内のすべての管理対象ホストに複製されます。

X-Force ルールは、IBM Security Threat Content アプリケーションが後でアンインストールされた場合でも、製品に表示されます。

手順

1. 「管理」タブで、「拡張の管理」をクリックします。
2. 以下のステップを実行して、IBM Security Threat Content アプリケーションを QRadar コンソールにアップロードします。
   a. 「追加」をクリックします。
   b. 「参照」をクリックし、参照して拡張を見つけます。
   c. オプション: 「即時にインストール」をクリックすると、コンテンツを表示せずに拡張をインストールできます。
   d. 「追加」をクリックします。
3. 拡張のコンテンツを表示するには、拡張のリストからその拡張を選択し、「詳細」をクリックします。
4. 拡張をインストールするには、以下の手順に従います。
   a. リストから拡張を選択し、「インストール」をクリックします。
   b. 拡張にデジタル署名が含まれていない場合、または署名がある一方で、その署名が IBM Security Certificate Authority (CA) に関連付けられていない場合は、それでもなおその拡張をインストールすることを確認する必要があります。インストールを続行する場合は、「インストール」をクリックします。
   c. インストールにより行われるシステムの変更を確認します。

d. 「上書き」または「既存データを保持」を選択して、既存のコンテンツ項目の処理方法を指定します。

e. 「インストール」をクリックします。

f. インストール・サマリーを確認し、「**OK**」をクリックします。

「ルール・リスト」ウィンドウの「脅威」グループの下にルールが表示されます。ルールは、使用する前に有効にする必要があります。

次のタスク

X-Force ルールを使用したり X-Force 機能を AQL 検索に追加したりできるように、X-Force Threat Intelligence フィードを有効にします。詳しくは、 201 ページの『X-Force Threat Intelligence フィードの有効化』を参照してください。

QRadar 用の IBM X-Force Exchange プラグイン

IBM X-Force Exchange (XFE) は、脅威情報の共有プラットフォームであり、セキュリティー分析者、ネットワーク・セキュリティーの専門家、およびセキュリティー・オペレーション・センターのチームが使用します。

XFE プラグインを使用して、以下の項目を検索できます。

- IP アドレス
- URL
- CVE
- Web アプリケーション

セキュリティー問題の調査時に見つかった情報を保管するリポジトリーである、公開コレクションや非公開コレクションに寄与することもできます。

また、コレクションには、Wiki スタイルのノートパッドとして機能するセクションが含まれています。このセクションに、関連するコメントやフリー・テキストを追加できます。コレクションを使用して、X-Force のレポート、テキスト・コメント、またはその他の任意の内容を保存できます。X-Force レポートには、保存した時点のバージョンのレポートと、現在のバージョンのレポートへのリンクの両方が含まれます。

このプラグインは、QRadar で見つかった IP アドレスについて、IBM X-Force Exchange Web サイトで情報を検索するためのオプションを提供します。イベントの URL を右クリックすると、特定の URL について X-Force Exchange が格納しているデータを確認できます。また、右クリックのルックアップ・オプションを使用すると、QRadar の検索、オフェンス、およびルールからの IP アドレスまたは URL データをコレクションに送信したり、それらのデータを使用してさらに調査したりできます。

IBM X-Force Exchange 右クリック・プラグインのインストール

IBM X-Force Exchange 右クリック・プラグインを IBM Fix Central からダウンロードすることで、QRadar コンソールにインストールします。

始める前に

この手順では、RPM がインストールされた後にプラグインをロードするために、「管理」タブから Web サーバーの再始動が必要です。Web サーバーを再始動すると、すべての QRadar ユーザーがログアウトされるため、定期保守の間にこのプラグインをインストールすることをお勧めします。

このタスクについて

QRadar システムがバージョン 7.2.3 以降である場合、このプラグインは既にインストール済みです。管理者は、QRadar 内の任意の IP アドレス上で右クリックして、「その他のオプション」 > 「プラグイン・オプション」を選択することで、プラグインがインストールされていることを確認できます。IBM X-Force Exchange ルックアップが表示される場合は、プラグインはインストールされています。

手順

1. X-Force Exchange 右クリック・プラグインを IBM Fix Central (https://ibm.biz/BdX4BW) からダウンロードします。
   a. RPM ファイルを QRadar コンソールにコピーします。
   b. コマンド `rpm -Uvh RightClick-XFE-7.2.<version>.x86_64.rpm` を入力して、プラグインをインストールします。
2. QRadar コンソールに管理ユーザーとしてログインします。
3. 「管理」タブをクリックします。
4. 「拡張」 > 「**Web** サーバーの再始動」を選択します。 Web サーバーの再始動後、X-Force 右クリック・プラグインは、「ログ・アクティビティー」タブの URL フィールドの QRadar 内の IP アドレスに対して有効になります。
5. 自分の IBMid を使用して X-Force Exchange Web サイトのポップアップ・ウィンドウにログインするか、ゲストとして続行します。 ゲスト・ユーザーは、X-Force Exchange Web サイトの一部の機能を使用できません。
6. IBM X-Force Exchange Web サイトへの初回ログインの後、ブラウザー・ウィンドウを閉じます。

X-Force Threat Intelligence フィードの有効化

IBM Security Threat Content アプリケーションでインストールされる拡張コンテンツを使用する前に、X-Force Threat Intelligence フィードを有効にする必要があります。

このタスクについて

X-Force Threat Intelligence フィードを有効にすると、QRadar は、1 日あたり約 30 MB の IP レピュテーション・データをダウンロードします。

手順

1. 「管理」タブで、「システム設定」をクリックします。
2. 「**X-Force Threat Intelligence** フィードの有効化」フィールドで「はい」を選択します。

次のタスク

X-Force サーバーからデータを受信するためにシステム設定の変更をデプロイします。詳しくは、『変更のデプロイ』を参照してください。

プロキシー・サーバー内の X-Force データの更新

IBM Security QRadar は、Apache サーバーを介したリバース・プロキシー・ルックアップを使用して、インターネット上の IBM Security X-Force Threat Intelligence サーバーから直接データを収集します。

このタスクについて

デプロイメント内のすべての QRadar アプライアンスは Apache サーバーに接続し、キャッシュされた要求を送信します。IBM Security QRadar コンソールによってデータが受信されると、結果がキャッシュに入れられ、新しい IP レピュテーション・データを要求する他のすべての管理対象ホストに結果が再生されます。

ネットワーク内でプロキシーが構成されている場合、X-Force データを受信するようにその構成を更新する必要があります。

制約事項: NTLM 認証はサポートされません。

手順

1. SSH を使用して QRadar コンソールにログインします。
2. テキスト・エディターで `/etc/httpd/conf.d/ssl.conf` ファイルを開きます。
3. `</VirtualHost>` の前に以下の行を追加します。

   ```
   ProxyRemote https://license.xforce-security.com/ http://
   PROXY_IP:PROXY_PORT

   ProxyRemote https://update.xforce-security.com/ http://
   PROXY_IP:PROXY_PORT
   ```
4. 会社のプロキシー・サーバーの IP アドレスとポートを更新して、X-Force セキュリティー・サーバーへの匿名接続ができるようにします。
5. `ssl.conf` ファイルへの変更を保存します。
6. 以下のコマンドを入力して Apache サーバーを再始動します。

   ```
   apachectl restart
   ```

   QRadar コンソールで Apache サーバーを再始動すると、すべてのユーザーがログアウトされ、管理対象ホストでエラー・メッセージが生成される場合があります。 Apache サーバーの再始動は、定期保守の間に行ってください。

ローカルでの X-Force データ・ダウンロードの停止

QRadar がローカル・システムに X-Force データをダウンロードするのを停止する場合は、「**X-Force Threat Intelligence** フィードの有効化」システム設定を無効にします。

X-Force フィードを無効にする前に、X-Force ルールが無効化されていること、および保存済み検索で X-Force 機能を使用してないことを確認してください。

X-Force コンテンツは、X-Force Threat Intelligence フィードを無効にした後も製品インターフェースに表示されます。フィードが無効になっているときは、X-Force ルールを使用することも X-Force 機能を AQL 検索に追加することもできません。

注:

「脅威およびセキュリティーのモニター」ダッシュボードの「インターネット脅威インフォメーション・センター」ウィジェットは、X-Force からの組み込み RSS フィードを使用します。X-Force からの日次脅威レベルおよび注意情報を表示するためにこのウィジェットが必要とすることは、QRadar がインターネットに接続していることのみです。X-Force Threat Intelligence フィードを有効にする必要はありません。

第 11 章 許可サービスの管理

IBM Security QRadar デプロイメント向けに API 呼び出しを認証するように、「管理」タブで許可サービスを構成できます。

QRadar RESTful API は許可サービスを使用して、QRadar コンソールへの API 呼び出しを認証します。いつでも許可サービスを追加または取り消すことができます。RESTful API について詳しくは、「*IBM Security QRadar API ガイド*」を参照してください。

「許可サービスの管理」ウィンドウは以下の情報を提供します。

表 *42.* 許可サービス用のパラメーター

パラメーター	説明
サービス名	許可サービスの名前。
権限を与えたユーザー	サービスの追加を許可したユーザーまたは管理者の名前。
認証トークン	この許可サービスに関連付けられたトークン。
ユーザー・ロール	この許可サービスに関連付けられたユーザー・ロール。
セキュリティー・プロファイル	当該の許可サービスと関連付けられているセキュリティー・プロファイル。
作成	この許可サービスが作成された日付。
有効期限	許可サービスの有効期限が切れる日付と時刻。デフォルトでは、許可サービスは 30 日間有効です。

関連概念:

5 ページの『IBM Security QRadar 製品の機能』
IBM Security QRadar 製品資料では、オフェンス、フロー、アセット、ヒストリカル相関などの機能について説明していますが、すべての QRadar 製品でこれらの機能を利用できるわけではありません。使用する製品によっては、説明されている一部の機能をデプロイメントで使用できない場合があります。各製品の機能を確認して、必要な情報を入手してください。

許可サービスの表示

「許可サービス」ウィンドウは許可サービスのリストを表示します。このリストからサービスのトークンをコピーできます。

手順

1. 「管理」タブをクリックします。
2. ナビゲーション・メニューで、「システム構成」をクリックします。
3. 「許可サービス」をクリックします。

4. 「許可サービスの管理」ウィンドウから、適切な許可サービスを選択します。

   このトークンは、最上部のバーの「選択されたトークン **(Selected Token)**」フィールドに表示されます。トークンをベンダー・ソフトウェアにコピーして、IBM Security QRadar で認証することができます。

許可サービスの追加

「許可サービスの追加」ウィンドウを使用して新規許可サービスを追加します。

手順

1. 「管理」タブをクリックします。
2. ナビゲーション・メニューで、「システム構成」をクリックします。
3. 「許可サービス」をクリックします。
4. 「許可サービスの追加」をクリックします。
5. 「サービス名」フィールドにこの許可サービスの名前を入力します。名前の長さは 255 文字まで可能です。
6. 「ユーザー・ロール」リストで、この許可サービスに割り当てたいユーザー・ロールを選択します。許可サービスに割り当てられたユーザー・ロールにより、その許可サービスが IBM Security QRadar のユーザー・インターフェース上でアクセスできる機能が決まります。
7. 「セキュリティー・プロファイル」リストで、この許可サービスに割り当てるセキュリティー・プロファイルを選択します。セキュリティー・プロファイルは、当該サービスが QRadar ユーザー・インターフェースでアクセスできるネットワークおよびログ・ソースを決定します。
8. 「有効期限日付」リストで、このサービスが期限切れになる日付を入力または選択します。有効期限を指定する必要がない場合は、「期限なし」を選択します。
9. 「サービスの作成」をクリックします。

   確認メッセージには、QRadar を使用して、ベンダー・ソフトウェアにコピーし、認証する必要のあるトークン・フィールドが含まれています。

許可サービスの取り消し

「許可サービスの追加」ウィンドウを使用して許可サービスを取り消します。

手順

1. 「管理」タブをクリックします。
2. ナビゲーション・メニューで、「システム構成」をクリックします。
3. 「許可サービス」をクリックします。
4. 「許可サービスの管理」ウィンドウから、取り消す許可サービスを選択します。
5. 「許可の取り消し **(Revoke Authorization)**」をクリックします。

第 12 章 バックアップおよびリカバリー

バックアップおよびリカバリーの機能を使用してイベント・データとフロー・データをバックアップすることで、IBM Security QRadar の構成情報とデータをバックアップおよびリカバリーできます。ただし、イベント・データおよびフロー・データのリストアは手動で行う必要があります。

バックアップのタイプには、構成バックアップとデータ・バックアップの 2 つがあります。詳しくは、 221 ページの『データのリストア』を参照してください。

デフォルトでは、QRadar は毎日真夜中に構成情報のバックアップ・アーカイブを作成します。構成バックアップは QRadar コンソールにのみ保管され、以下の情報が含まれます。

- アプリケーションの構成
- アセット
- 証明書
- カスタム・ロゴ
- カスタム・ルール
- デバイス・サポート・モジュール (DSM)
- イベント・カテゴリー
- フロー・ソース
- フロー検索とイベント検索
- グループ
- 索引管理情報
- ライセンス・キー情報
- ログ・ソース
- オフェンス
- リファレンス・セット・エレメント
- ストア・アンド・フォワード・スケジュール
- ユーザー情報とユーザー・ロール情報
- 脆弱性データ (IBM Security QRadar Vulnerability Manager がインストールされている場合)

データ・バックアップには以下の情報が含まれます。

- 監査ログ情報
- イベント・データ
- フロー・データ
- レポート・データ
- 索引

QRadar コンソールを含め、デプロイメント環境の各管理対象ホストでは、日次のデータ・バックアップ・ファイルをローカルに作成して保管します。データ・バックアップ・アーカイブは毎日作成され、前日のイベント・データとフロー・データが含まれます。日次バックアップのサイズは、前日から受け取ったイベント・データの量に応じて異なります。

バックアップ・ファイルのデフォルトの場所は、/store/backup/ ディレクトリーです。ご使用のシステムには、外部の SAN または NAS サービスからの /store/backup マウントがある場合もあります。外部サービスにより、データをオフラインで長期にわたって保存できるようになっています。これは通常、規制 (PCI など) の準拠に必要となります。

データ・バックアップにはアプリケーション・データは含まれません。アプリケーション・データのバックアップを構成および管理するには、 225 ページの『アプリケーション・データのバックアップおよびリストア』を参照してください。

関連概念:

5 ページの『IBM Security QRadar 製品の機能』
IBM Security QRadar 製品資料では、オフェンス、フロー、アセット、ヒストリカル相関などの機能について説明していますが、すべての QRadar 製品でこれらの機能を利用できるわけではありません。使用する製品によっては、説明されている一部の機能をデプロイメントで使用できない場合があります。各製品の機能を確認して、必要な情報を入手してください。

関連タスク:

221 ページの『データのリストア』
IBM Security QRadar コンソールおよび管理対象ホストのデータを、バックアップ・ファイルからリストアできます。バックアップ・ファイルのデータ部分には、送信元および宛先の IP アドレス情報、アセット・データ、イベント・カテゴリー情報、脆弱性データ、フロー・データ、イベント・データなどの情報が含まれています。

QRadar の構成およびデータのバックアップ

デフォルトでは、IBM Security QRadar は毎日真夜中に構成情報のバックアップ・アーカイブを作成します。バックアップ・アーカイブには、その前日の構成情報またはデータ、あるいはその両方が含まれます。必要に応じて、この毎晩のバックアップをカスタマイズし、オンデマンドの構成バックアップを作成できます。

毎晩のバックアップのスケジュール

「バックアップ・リカバリー構成」ウィンドウを使用して、夜間にスケジュールされるバックアップ・プロセスを構成します。

このタスクについて

デフォルトでは、毎晩のバックアップ・プロセスには構成ファイルのみが含まれています。IBM Security QRadar コンソールのデータと選択された管理対象ホストを含めるように毎晩のバックアップ・プロセスをカスタマイズできます。また、バックアップ保存期間、バックアップ・アーカイブのロケーション、タイムアウト前の

バックアップ処理の時間制限、およびその他の QRadar プロセスに関連するバックアップの優先順位についてカスタマイズすることもできます。

注**:** 最適なパフォーマンスを実現するために、QRadar の自動更新と同時に毎晩のバックアップをスケジュールしないことをお勧めします。

「バックアップ・リカバリー構成」ウィンドウには、以下のパラメーターが用意されています。

表 *43.* 「バックアップ・リカバリー構成」パラメーター

パラメーター	説明
一般バックアップ構成	
バックアップ・リポジトリー・パス (Backup Repository Path)	バックアップ・ファイルを保管するロケーションを入力します。デフォルト・ロケーションは /store/backup です。このパスは、バックアップ・プロセスが開始される前に存在している必要があります。このパスが存在しない場合は、バックアップ・プロセスが異常終了します。 このパスを変更する場合は、必ず、新しいパスがデプロイメントのすべてのシステム上で有効であるようにしてください。 • アクティブ・データは /store ディレクトリーに保管されます。アクティブ・データとバックアップ・アーカイブがともに同じディレクトリーに保管されている場合、データ・ストレージは容易に最大容量に達する可能性があり、スケジュールされたバックアップは失敗することがあります。ストレージ・ロケーションを別のシステム上に指定するか、バックアップ・プロセスの完了後にバックアップ・アーカイブを別のシステムにコピーすることをお勧めします。QRadar デプロイメントでネットワーク・ファイル・システム (NFS) ストレージ・ソリューションを使用できます。NFS の使用について詳しくは、「オフボード・ストレージ・ガイド」を参照してください。
バックアップ保存期間 (日)	バックアップ・ファイルを保管する期間 (日) を入力するか選択します。デフォルトは、2 日間です。 この期間は、スケジュールされたプロセスの結果として生成されるバックアップ・ファイルのみに影響を与えます。オンデマンド・バックアップまたはインポートされたバックアップ・ファイルはこの値の影響を受けません。

表 43. 「バックアップ・リカバリー構成」パラメーター (続き)

パラメーター	説明
毎晩のバックアップのスケジュール (Nightly Backup Schedule)	バックアップ・オプションを選択します。
データ・バックアップを実行する管理対象ホストの選択	このオプションは、「構成バックアップとデータ・バックアップ **(Configuration and Data Backups)**」オプションを選択した場合のみ表示されます。 デプロイメント内のすべてのホストがリストされます。リスト内の最初のホストはコンソールです。デフォルトでは、最初のホストはデータ・バックアップが有効化されているため、チェック・ボックスは表示されません。デプロイメント内に管理対象ホストがある場合、管理対象ホストはコンソールの下にリストされ、各管理対象ホストにはチェック・ボックスが表示されます。 データ・バックアップを実行する管理対象ホストのチェック・ボックスを選択します。 ホスト (コンソールまたは管理対象ホスト) ごとに、バックアップ・アーカイブから除外するデータ項目をオプションでクリアできます。
構成のみのバックアップ	
バックアップ時間制限 (分)	バックアップに使用する時間 (分) を入力するか選択します。デフォルトは、180 分です。バックアップ・プロセスは、構成された時間制限を超えた場合、自動的にキャンセルされます。
バックアップ優先順位	このリスト・ボックスから、他のプロセスと比較してシステムに指定する、構成バックアップ・プロセスの重要度を選択します。 優先順位が中または高の場合は、システム・パフォーマンスへの影響が大きくなります。
データ・バックアップ	
バックアップ時間制限 (分)	バックアップに使用する時間 (分) を入力するか選択します。デフォルトは、1020 分です。バックアップ・プロセスは、構成された時間制限を超えた場合、自動的にキャンセルされます。

表 43. 「バックアップ・リカバリー構成」パラメーター (続き)

パラメーター	説明
バックアップ優先順位	リストから、他のプロセスと比較してシステムに指定する、データ・バックアップ・プロセスの重要度を選択します。 優先順位が中または高の場合は、システム・パフォーマンスへの影響が大きくなります。

手順

1. 「管理」タブをクリックします。
2. ナビゲーション・メニューで、「システム構成」をクリックします。
3. 「バックアップおよびリカバリー **(Backup and Recovery)**」アイコンをクリックします。
4. ツールバーで、「構成」をクリックします。
5. 「バックアップ・リカバリー構成」ウィンドウで、毎晩のバックアップをカスタマイズします。
6. 「保存」をクリックします。
7. 「アーカイブのバックアップ」ウィンドウを閉じます。
8. 「管理」タブ・メニューで、「変更のデプロイ」をクリックします。

オンデマンド構成バックアップ・アーカイブの作成

夜間にスケジュールしたバックアップ以外の時刻に構成ファイルをバックアップする必要がある場合、オンデマンド・バックアップ・アーカイブを作成できます。オンデマンド・バックアップ・アーカイブには、構成情報のみが格納されます。

このタスクについて

IBM Security QRadar の処理負荷が低い場合 (通常の営業時間の後など) の時にオンデマンド・バックアップ・アーカイブを開始します。バックアップ・プロセス中は、システム・パフォーマンスが影響を受けます。

手順

1. 「管理」タブをクリックします。
2. ナビゲーション・メニューで、「システム構成」をクリックします。
3. 「バックアップおよびリカバリー」をクリックします。
4. ツールバーから、「オンデマンド・バックアップ **(On Demand Backup)**」をクリックします。
5. 以下のパラメーターの値を入力します。

オプション	説明
名前	このバックアップ・アーカイブに割り当てる固有の名前を入力します。名前の長さは英数字 100 文字まで可能です。名前にはアンダースコアー (_)、ダッシュ (-)、またはピリオド (.) を含めることができます。
説明	この構成バックアップ・アーカイブの説明を入力します。説明の長さは 255 文字まで可能です。

6. 「バックアップの実行 **(Run Backup)**」をクリックします。

新規のバックアップ・プロセスまたはリストア・プロセスを開始できるのは、オンデマンド・バックアップが完了してからのみです。バックアップ・アーカイブ・プロセスは、「アーカイブのバックアップ」ウィンドウでモニターできます。 215 ページの『バックアップ・アーカイブの表示』を参照してください。

バックアップが失敗した場合の E メール通知の作成

IBM Security QRadar コンソールまたは QRadar Event Processor でのバックアップの失敗に関する通知を E メールで受け取るには、システム通知メッセージに基づくルールを作成します。

始める前に

QRadar でシステム通知を配布するための E メール・サーバーを構成する必要があります。詳しくは、 79 ページの『ローカル・ファイアウォールの構成』を参照してください。

このタスクについて

バックアップが失敗すると、以下のいずれかのバックアップ障害システム通知が表示されます。

- バックアップにより多くのディスク・スペースが必要 (Backup requires more disk space)
- バックアップ: 最後のバックアップが実行のしきい値を超えた (Backup: last Backup exceeded execution threshold)
- バックアップで要求を実行できない (Backup unable to execute request)

手順

1. 「オフェンス」タブをクリックします。
2. 「オフェンス」ペインで、「ルール」をクリックします。
3. 「アクション」 > 「新規イベント・ルール」をクリックします。
4. 「ルール・ウィザード」で、「ルール・ウィザードの実行時にこのページをスキップする」チェック・ボックスにチェック・マークを付けて、「次へ」をクリックします。
5. フィルター・ボックスに以下の検索照会を入力します。

イベント QID が以下のいずれかの QID である場合 (when the event QID is one of the following QIDs)

テストに関する詳細の説明:

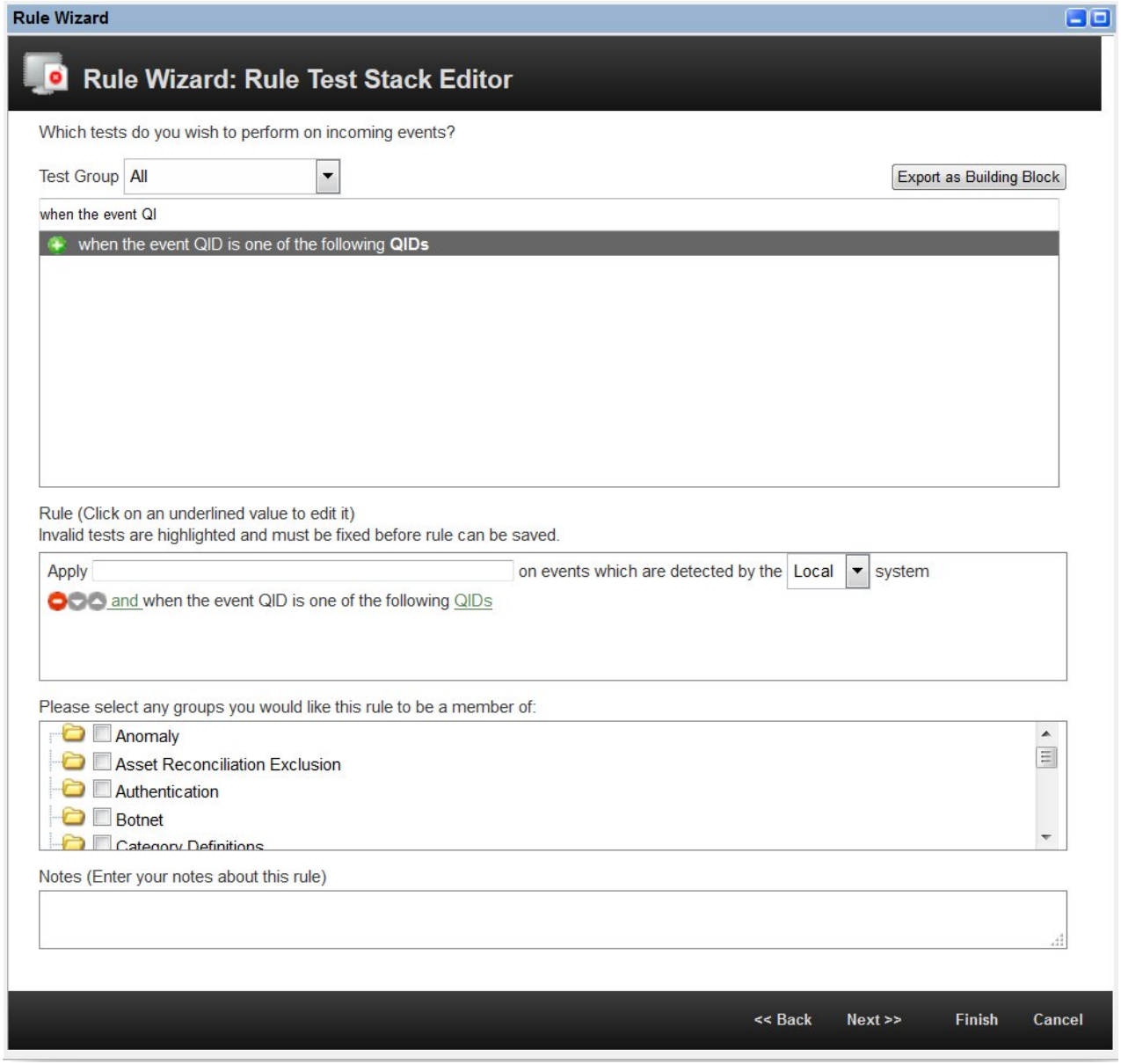


図 7. 「ルール・ウィザード」イベント・テスト

6. 緑色の追加アイコン **(+)** をクリックします。
7. 「ルール」ペインで、「**QID**」リンクをクリックします。
8. 「**QID/名前**」フィールドに**バックアップ** (Backup): と入力します。
9. 以下の QID を選択し、「追加 **+**」をクリックします。
   - バックアップにより多くのディスク・スペースが必要 **(Backup requires more disk space)**

- バックアップ**:** 最後のバックアップが実行のしきい値を超えた **(Backup: last backup exceeded execution threshold)**
- バックアップで要求を実行できない **(Backup unable to execute request)**

QID に関する詳細の説明**:**

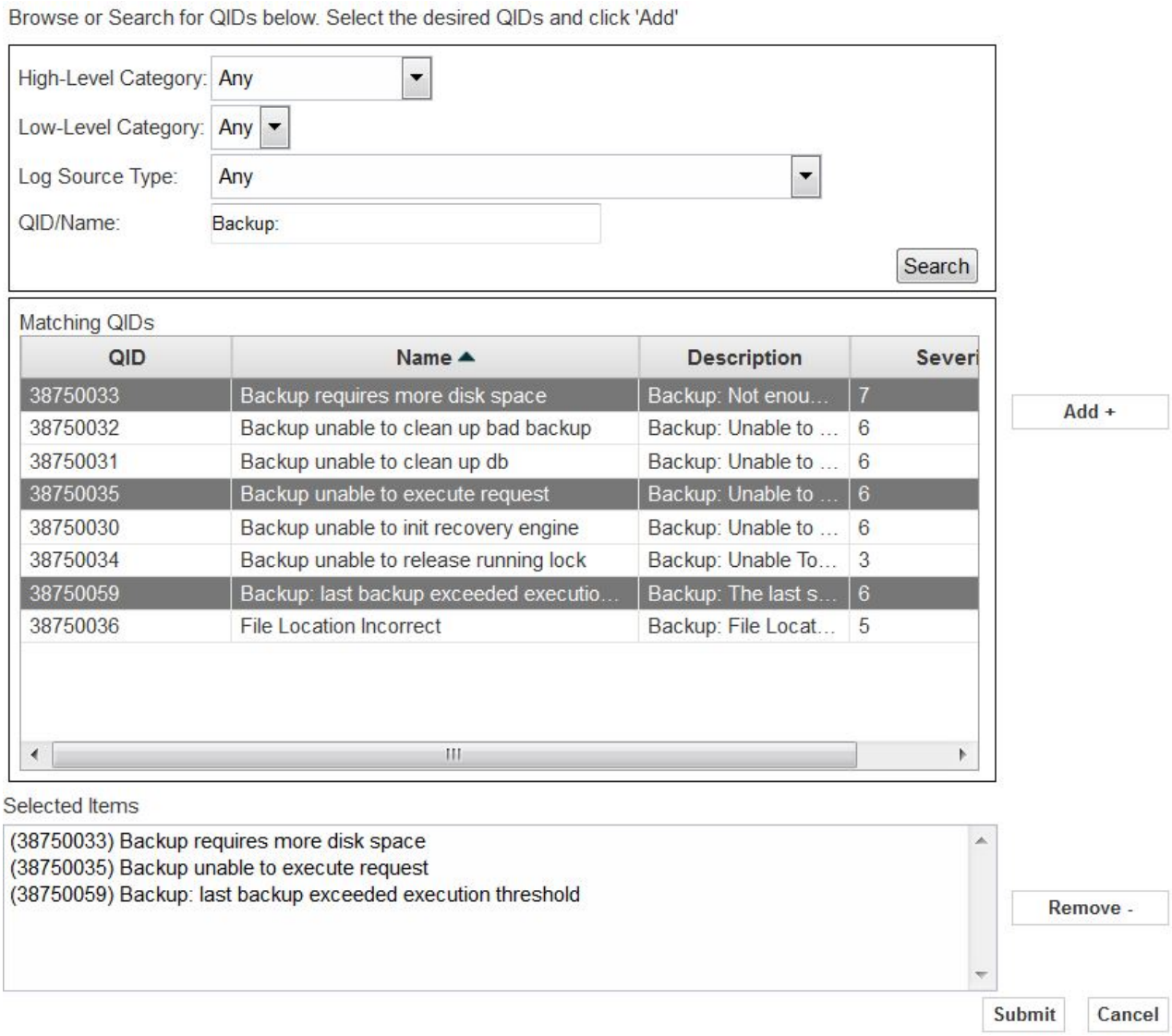


図 *8.* 「ルール・ウィザード」の *QID*

10. 「送信 **(Submit)**」をクリックします。
11. 「ルール」ペインで、ルール・テストに以下の名前を入力し、「次へ」をクリックします。

    バックアップ障害 (Backup Failure)
12. 「ルールの応答」セクションで、「**E** メール」ボックスにチェック・マークを付け、通知先とする E メール・アドレスを入力します。

既存のバックアップ・アーカイブの管理

成功したすべてのバックアップ・アーカイブを表示したり管理したりするには、「アーカイブのバックアップ」ウィンドウを使用します。

バックアップ・アーカイブの表示

「アーカイブのバックアップ」ウィンドウを使用してバックアップ・アーカイブのリストを表示します。

手順

1. 「管理」タブをクリックします。
2. ナビゲーション・メニューで、「システム構成」をクリックします。
3. 「バックアップおよびリカバリー」をクリックします。

バックアップ・アーカイブのインポート

バックアップ・アーカイブのインポートが役立つのは、別の IBM Security QRadar ホスト上に作成されたバックアップ・アーカイブをリストアする場合です。

このタスクについて

QRadar バックアップ・アーカイブ・ファイルをコンソール・サーバーの `/store/backupHost/inbound` ディレクトリーに配置した場合、バックアップ・アーカイブ・ファイルは自動的にインポートされます。

手順

1. 「管理」タブをクリックします。
2. ナビゲーション・メニューで、「システム構成」をクリックします。
3. 「バックアップおよびリカバリー **(Backup and Recovery)**」アイコンをクリックします。
4. 「アーカイブのアップロード **(Upload Archive)**」フィールドで、「参照 **(Browse)**」をクリックします。
5. アップロードするアーカイブ・ファイルを見つけて選択します。アーカイブ・ファイル名には `.tgz` 拡張子が含まれている必要があります。
6. 「オープン」をクリックします。
7. 「アップロード」をクリックします。

バックアップ・アーカイブの削除

バックアップ・アーカイブ・ファイルを削除するには、バックアップ・アーカイブ・ファイルとホスト・コンテキスト・コンポーネントが同じシステム上に配置されている必要があります。また、システムは IBM Security QRadar コンソールと通信中であることが必要で、その他のバックアップは進行できません。

このタスクについて

バックアップ・ファイルを削除すると、ディスクとデータベースから削除されます。また、エントリーがこのリストから削除され、削除を示す監査イベントが生成されます。

手順

1. 「管理」タブをクリックします。
2. ナビゲーション・メニューで、「システム構成」をクリックします。
3. 「バックアップおよびリカバリー」をクリックします。
4. 「既存のバックアップ」セクションで、削除するアーカイブを選択します。
5. 「削除」をクリックします。

QRadar の構成およびデータのリストア

以前にアーカイブされた構成ファイル、オフェンス・データ、およびアセット・データを IBM Security QRadar システムにリストアする場合は、バックアップ・アーカイブのリストアが便利です。

バックアップ・アーカイブをリストアする前に、以下の考慮事項に注意してください。

- ソフトウェアの同じリリース (パッチ・レベルを含む) 内で作成されたバックアップ・アーカイブのみをリストアできます。例えば、QRadar 7.1.0 (MR2) を実行している場合、バックアップ・アーカイブは QRadar で作成されている必要があります。
- リストア・プロセスでは、構成情報、オフェンス・データ、およびアセット・データのみがリストアされます。詳しくは、 221 ページの『データのリストア』を参照してください。
- バックアップ・アーカイブが NATed Console システムで作成されている場合、そのバックアップ・アーカイブは NATed システムにのみリストアできます。

リストア・プロセス中は以下のステップがコンソールで行われます。

1. 既存のファイルおよびデータベース表がバックアップされます。
2. Tomcat がシャットダウンされます。
3. すべてのシステム・プロセスがシャットダウンされます。
4. ファイルがバックアップ・アーカイブから抽出され、ディスクにリストアされます。
5. データベース表がリストアされます。
6. すべてのシステム・プロセスが再開されます。
7. Tomcat が再始動されます。

関連タスク:

221 ページの『データのリストア』

IBM Security QRadar コンソールおよび管理対象ホストのデータを、バックアップ・ファイルからリストアできます。バックアップ・ファイルのデータ部分には、送信元および宛先の IP アドレス情報、アセット・データ、イベント・カテゴリー情報、脆弱性データ、フロー・データ、イベント・データなどの情報が含まれています。

バックアップ・アーカイブのリストア

バックアップ・アーカイブをリストアできます。バックアップ・アーカイブのリストアが役立つのは、システム・ハードウェア障害が発生した場合や、バックアップ・アーカイブを交換アプライアンスに保管する場合です。

このタスクについて

リストア・プロセスが完了するまで、コンソールを再始動することはできません。

リストア・プロセスには数時間かかることがあります (処理時間は、リストア対象のバックアップ・アーカイブのサイズに依存します)。完了すると、確認メッセージが表示されます。

ウィンドウはリストア・プロセスの状況を示します。このウィンドウには、各ホストのエラーとエラーを解決する指示がすべて示されます。

「バックアップのリストア」ウィンドウでは、以下のパラメーターが使用可能です。

表 *44.* 「バックアップのリストア」パラメーター

パラメーター	説明
名前	バックアップ・アーカイブの名前。
説明	バックアップ・アーカイブの説明がある場合。
タイプ	バックアップのタイプ。構成バックアップのみをリストアできるため、このパラメーターは「構成 **(config)**」を表示します。
すべての構成項目を選択 **(Select All Configuration Items)**	このオプションを選択した場合、すべての構成項目がバックアップ・アーカイブのリストアに含まれることを意味します。
構成のリストア **(Restore Configuration)**	バックアップ・アーカイブのリストアに含める構成項目をリストします。項目を削除するには、削除する項目ごとにチェック・ボックスをクリアするか、「すべての構成項目を選択 **(Select All Configuration Items)**」チェック・ボックスをクリアします。
すべてのデータ項目を選択 **(Select All Data Items)**	このオプションを選択した場合、すべてのデータ項目がバックアップ・アーカイブのリストアに含まれることを意味します。
リストア・データ **(Restore Data)**	バックアップ・アーカイブのリストアに含める構成項目をリストします。デフォルトではすべての項目がクリアされています。データ項目をリストアするには、リストアする項目ごとにチェック・ボックスを選択できます。

手順

1. 「管理」タブをクリックします。
2. ナビゲーション・メニューで、「システム構成」をクリックします。

3. 「バックアップおよびリカバリー **(Backup and Recovery)**」アイコンをクリックします。
4. リストアするアーカイブを選択します。
5. 「リストア」をクリックします。
6. 「バックアップのリストア」ウィンドウで、パラメーターを構成します。

   注**:** 「インストール済みアプリケーションの構成」チェック・ボックスを選択することで、インストール済みアプリケーションの構成のみをリストアします。拡張の構成はリストアされません。拡張の構成をリストアする場合は、「デプロイメント構成」チェック・ボックスを選択します。
7. 「リストア」をクリックします。
8. 「**OK**」をクリックします。
9. 「**OK**」をクリックします。
10. 次のオプションのいずれかを選択してください。
    - ユーザー・インターフェースがリストア・プロセス中に閉じた場合は、Web ブラウザーを開いて IBM Security QRadar にログインします。
    - ユーザー・インターフェースが閉じられていない場合は、ログイン・ウィンドウが表示されます。QRadar にログインします。
11. 状況ウィンドウの説明に従います。

次のタスク

システムにデータがリストアされたことを確認後、DSM、脆弱性評価 (VA) スキャナー、およびログ・ソース・プロトコルもリストアされていることを確認します。

バックアップ・アーカイブが HA クラスターで作成されている場合、リストアが完了した後、「変更のデプロイ」をクリックして HA クラスター構成をリストアする必要があります。ディスク複製が有効の場合、システムがリストアされた後、セカンダリー・ホストは即時にデータを同期します。バックアップ後にセカンダリー・ホストがデプロイメントから削除された場合、セカンダリー・ホストは「システムおよびライセンス管理」ウィンドウに失敗状況を表示します。

別の QRadar システムに作成されたバックアップ・アーカイブのリストア

各バックアップ・アーカイブには、バックアップ・アーカイブ作成元のシステムの IP アドレス情報が含まれます。バックアップ・アーカイブを別の IBM Security QRadar システムからリストアすると、バックアップ・アーカイブの IP アドレスと、リストアしているシステムの IP アドレスは一致しません。一致しない IP アドレスを訂正することができます。

このタスクについて

リストア・プロセスが完了するまで、コンソールを再始動することはできません。

リストア・プロセスには数時間かかることがあります (処理時間は、リストア対象のバックアップ・アーカイブのサイズに依存します)。完了すると、確認メッセージが表示されます。

ウィンドウはリストア・プロセスの状況を示します。このウィンドウには、各ホストのエラーとエラーを解決する指示がすべて示されます。

デプロイメント内の各管理対象ホストで iptables サービスを停止する必要があります。iptables サービスは Linux ベースのファイアウォールです。

「バックアップのリストア (管理対象ホストのアクセス可能性)」ウィンドウは以下の情報を提供します。

表 *45.* 「バックアップのリストア *(*管理対象ホストのアクセス可能性*)*」パラメーター

パラメーター	説明
ホスト名	管理対象ホストの名前。
IP アドレス	管理対象ホストの IP アドレス。
アクセス状況 **(Access Status)**	管理対象ホストへのアクセス状況。

「バックアップのリストア」ウィンドウは以下のパラメーターを提供します。

表 *46.* 「バックアップのリストア」パラメーター

パラメーター	説明
名前	バックアップ・アーカイブの名前。
説明	バックアップ・アーカイブの説明がある場合。
タイプ	バックアップのタイプ。構成バックアップのみをリストアできるため、このパラメーターは「構成 **(config)**」を表示します。
すべての構成項目を選択 **(Select All Configuration Items)**	このオプションを選択した場合、すべての構成項目がバックアップ・アーカイブのリストアに含まれることを意味します。このチェック・ボックスはデフォルトで選択されています。すべての構成項目をクリアするには、チェック・ボックスをクリアします。
構成のリストア **(Restore Configuration)**	バックアップ・アーカイブのリストアに含める構成項目をリストします。デフォルトではすべての項目が選択されています。項目を削除するには、削除する項目ごとにチェック・ボックスをクリアするか、「すべての構成項目を選択 **(Select All Configuration Items)**」チェック・ボックスをクリアします。
すべてのデータ項目を選択 **(Select All Data Items)**	このオプションを選択した場合、すべてのデータ項目がバックアップ・アーカイブのリストアに含まれることを意味します。このチェック・ボックスはデフォルトで選択されています。すべてのデータ項目をクリアするには、このチェック・ボックスをクリアします。

表 46. 「バックアップのリストア」パラメーター (続き)

パラメーター	説明
リストア・データ **(Restore Data)**	バックアップ・アーカイブのリストアに含める構成項目をリストします。デフォルトではすべての項目がクリアされています。データ項目をリストアするには、リストアする項目ごとにチェック・ボックスを選択できます。

手順

1. 「管理」タブをクリックします。
2. ナビゲーション・メニューで、「システム構成」をクリックします。
3. 「バックアップおよびリカバリー **(Backup and Recovery)**」アイコンをクリックします。
4. リストアするアーカイブを選択します。
5. 「リストア」をクリックします。
6. 「バックアップのリストア」ウィンドウで、パラメーターを構成します。
7. 「リストア」をクリックします。
8. 以下のように iptables を停止します。
   a. SSH を使用して、管理対象ホストに root ユーザーとしてログインします。
   b. コマンド **service iptables stop** を入力します。
   c. デプロイメント内のすべての管理対象ホストにこの操作を繰り返します。
9. 「バックアップのリストア」ウィンドウで、「ホスト・アクセスのテスト **(Test Hosts Access)**」をクリックします。
10. すべての管理対象ホストのテストが完了したら、「アクセス状況 **(Access Status)**」列の状況が「**OK**」の状況を示していること確認します。
11. ホストの「アクセス状況 **(Access Status)**」列が「アクセスなし **(No Access)**」の状況を示している場合、iptables を再度停止してから、「ホスト・アクセスのテスト **(Test Host Access)**」を再度クリックして接続を試行します。
12. 「バックアップのリストア」ウィンドウで、パラメーターを構成します。

    注**:** 「インストール済みアプリケーションの構成」チェック・ボックスを選択することで、インストール済みアプリケーションの構成のみをリストアします。拡張の構成はリストアされません。拡張の構成をリストアする場合は、「デプロイメント構成」チェック・ボックスを選択します。
13. 「リストア」をクリックします。
14. 「**OK**」をクリックします。
15. 「**OK**」をクリックしてログインします。
16. 次のオプションのいずれかを選択してください。
    - ユーザー・インターフェースがリストア・プロセス中に閉じた場合は、Web ブラウザーを開いて QRadar にログインします。

- ユーザー・インターフェースを閉じなかった場合は、ログイン・ウィンドウが表示されます。QRadar にログインします。

17. リストア・プロセスの結果を表示し、エラーがある場合は解決する指示に従います。
18. Web ブラウザー・ウィンドウを最新表示します。
19. 「管理」タブから、「拡張」 > 「すべての構成のデプロイ」を選択します。

    完全構成をデプロイすると、QRadar によりすべてのサービスが再始動されます。イベントおよびフローに関するデータ収集は、デプロイが完了するまで停止します。

次のタスク

データがシステムにリストアされたことを確認した後、すべての DSM、脆弱性評価 (VA) スキャナー、またはログ・ソース・プロトコルについて RPM を再適用する必要があります。

バックアップ・アーカイブが HA クラスターで作成されている場合、リストアが完了した後、「変更のデプロイ」をクリックして HA クラスター構成をリストアする必要があります。ディスク複製が有効の場合、システムがリストアされた後、セカンダリー・ホストは即時にデータを同期します。バックアップ後にセカンダリー・ホストがデプロイメントから削除された場合、セカンダリー・ホストは「システムおよびライセンス管理」ウィンドウに失敗状況を表示します。

データのリストア

IBM Security QRadar コンソールおよび管理対象ホストのデータを、バックアップ・ファイルからリストアできます。バックアップ・ファイルのデータ部分には、送信元および宛先の IP アドレス情報、アセット・データ、イベント・カテゴリー情報、脆弱性データ、フロー・データ、イベント・データなどの情報が含まれています。

QRadar コンソールを含め、デプロイメント環境の各管理対象ホストでは、すべてのバックアップ・ファイルを `/store/backup/` ディレクトリーに作成します。ご使用のシステムには、外部の SAN または NAS サービスからの `/store/backup` マウントがある場合もあります。外部サービスにより、データをオフラインで長期にわたって保存できるようになっています。これは通常、規制 (PCI など) の準拠に必要となります。

制約事項**:** データのバックアップをリストアする前に、構成のバックアップをリストアしておく必要があります。

始める前に

以下の条件が満たされているようにします。

- 新規の QRadar コンソールにデータをリストアする場合は、構成のバックアップがリストアされている。
- データがバックアップされている管理対象ホストのロケーションが把握されている。

- デプロイメント環境にそのボリューム用のマウント・ポイントが別途存在する場合は、その /store ディレクトリーまたは /store/ariel ディレクトリーに、リカバリー対象のデータに対する十分なスペースがある。
- リカバリー対象のデータの日時が把握されている。

手順

1. SSH を使用して、root ユーザーとして IBM Security QRadar にログインします。
2. /store/backup ディレクトリーに移動します。
3. バックアップ・ファイルをリストするには、次のコマンドを入力します。

   ```
   ls -l
   ```

4. バックアップ・ファイルがリストされたら、次のコマンドを入力してルート・ディレクトリーに移動します。

   ```
   cd /
   ```

   重要: リストアされるファイルは /store ディレクトリーにある必要があります。 cd / でなく cd と入力した場合、ファイルは /root/store ディレクトリーにリストアされます。
5. バックアップ・ファイルを元のディレクトリーに抽出するには、以下のコマンドを入力します。

   ```
   tar -zxpvPf /store/backup/backup.name.hostname_hostID .target
   date.backup type.timestamp.tgz
   ```

表 47. ファイル名の変数についての説明

ファイル名の変数	説明
name	バックアップの名前。
hostname_hostID	バックアップ・ファイルをホストする QRadar システムの名前であり、その後に QRadar システムの ID が続きます。
target date	バックアップ・ファイルが作成された日付。対象とする日付の形式は、*day_month_year* です。
backup type	このオプションは、data または config となります。
timestamp	バックアップ・ファイルが作成された時刻。

タスクの結果

データの日次バックアップでは、各ホスト上のすべてのデータが取得されます。データをリストアする対象が、イベント・データまたはフロー・データのみを格納している管理対象ホストである場合、そのホストには当該データのみがリストアされます。リストアされたデータを維持するには、リストアされたデータが夜間のディスク保守ルーチンで削除されないよう、データの保存設定の値を大きくしてください。

関連概念:

207 ページの『第 12 章 バックアップおよびリカバリー』
バックアップおよびリカバリーの機能を使用してイベント・データとフロー・データをバックアップすることで、IBM Security QRadar の構成情報とデータをバックアップおよびリカバリーできます。ただし、イベント・データおよびフロー・データのリストアは手動で行う必要があります。

216 ページの『QRadar の構成およびデータのリストア』
以前にアーカイブされた構成ファイル、オフェンス・データ、およびアセット・データを IBM Security QRadar システムにリストアする場合は、バックアップ・アーカイブのリストアが便利です。

リストアされたデータの検証

データが正しく IBM Security QRadar にリストアされていることを検証します。

手順

1. ファイルがリストアされたことを検証するため、以下のコマンドを入力して、リストアされたディレクトリーのうちの 1 つの内容をレビューします。

   ```
   cd /store/ariel/flows/payloads/<yyyy/mm/dd>
   ```

   ```
   cd /store/ariel/events/payloads/<yyyy/mm/dd>
   ```

   該当日の 1 時間ごとに作成された、リストアされたディレクトリーを表示することができます。ディレクトリーが欠落している場合、その時間枠ではデータが収集されていない可能性があります。
2. リストアされたデータが使用可能であるかどうかを検証します。
   a. QRadar インターフェースにログインします。
   b. 「ログ・アクティビティー」タブまたは「ネットワーク・アクティビティー」タブをクリックします。
   c. ツールバーの「検索」リストから、「検索の編集」を選択します。
   d. 「検索」ウィンドウの「時刻範囲」ペインで、「特定の間隔」を選択します。
   e. リストアしたデータの時刻範囲を選択してから「フィルター」をクリックします。
   f. 結果を表示して、リストアしたデータについて検証します。
   g. リストアしたデータが QRadar インターフェースで使用不可になっている場合は、データが正しいロケーションにリストアされていること、さらにファイルの権限が正しく構成されていることを検証します。

      リストアされたファイルは /store ディレクトリーにある必要があります。リストアされたファイルを抽出する際に、cd / ではなく cd と入力した場合は、/root/store ディレクトリーでリストアされたファイルを確認します。リストアされたファイルを抽出する前にディレクトリーの変更をしなかった場合は、 /store/backup/store ディレクトリーでリストアされたファイルを確認します。

      通常、ファイルは元の権限のままリストアされます。ただし、ファイルを所有しているのが root ユーザー・アカウントである場合、問題が発生する場

合があります。ファイルを所有しているのが root ユーザー・アカウントである場合は、**chown** コマンドおよび **chmod** コマンドを使用して、権限を変更します。

次のタスク

データがリストアされたことを確認したら、すべての DSM、脆弱性評価 (VA) スキャナー、およびログ・ソース・プロトコルに対し、RPM を再適用する必要があります。

アプリケーションのバックアップとリストア

IBM Security QRadar には、アプリケーション・データとは別に、アプリケーションの構成をバックアップおよびリストアするための方法が用意されています。

アプリケーションの構成は、毎晩の構成バックアップの一環としてバックアップされます。構成バックアップには、QRadar コンソールにインストールされたアプリケーションと、アプリケーション・ノードにインストールされたアプリケーションが含まれます。バックアップのリストア時に「インストール済みアプリケーションの構成」オプションを選択することにより、アプリケーションの構成をリストアできます。

アプリケーション・データは、使いやすいスクリプトを使用して、アプリケーションの構成とは別にバックアップされます。このスクリプトは毎晩実行されます。また、このスクリプトを使用して、アプリケーション・データをリストアしたり、アプリケーション・データのバックアップ時間およびデータ保存期間を構成したりすることもできます。

関連概念:

138 ページの『アプリケーション・ノード』
アプリケーション・ノードをプロビジョンすることで、QRadar コンソールの処理能力に影響を与えずに、アプリケーション用の追加のストレージ、メモリー、および CPU リソースを提供します。UBA (User Behavior Analytics) などのアプリケーションは、QRadar コンソールで現在使用できるリソースより多くのリソースを必要とします。

アプリケーションのバックアップおよびリストア

「管理」タブの IBM Security QRadar の「バックアップおよびリカバリー」ウィンドウを使用して、アプリケーションのバックアップおよびリストアを行います。

このタスクについて

構成バックアップを作成することで、アプリケーションをバックアップできます。構成バックアップでは、アプリケーションのデータはバックアップされません。

アプリケーション・ノードが QRadar コンソールに接続されている場合、そのアプリケーション・ノードの構成は、コンソールのデプロイメント構成の一部としてバックアップされます。アプリケーション・ノードが当初に構成された IP アドレスとは異なる IP アドレスで、 QRadar コンソールでそのアプリケーション・ノードをリストアすることはできません。

アプリケーションは、アプリケーション・ノードが存在している場合を除き、デフォルトでコンソールにリストアされます。QRadar は、アプリケーションをアプリケーション・ノードにリストアできない場合、QRadar コンソールへのリストアを試行します。コンソールにリストアできるアプリケーション・ノードのアプリケーションの数は、QRadar コンソールで使用可能なメモリー量によって制限されます。アプリケーションのアプリケーション・マニフェスト・ファイルで **node_only** と定義されているアプリケーションは、QRadar コンソールにリストアできません。

手順

1. 「管理」タブで「バックアップおよびリカバリー」をクリックします。
2. 「バックアップおよびリカバリー」ウィンドウ内の既存のバックアップを選択して、「リストア」をクリックします。
3. 「インストール済みアプリケーションの構成」チェック・ボックスが選択されていることを確認して、「リストア」をクリックします。

   注: 「インストール済みアプリケーションの構成」チェック・ボックスを選択することで、インストール済みアプリケーションの構成のみをリストアします。拡張の構成は、リストアされません。拡張の構成をリストアする場合は、「デプロイメント構成」チェック・ボックスを選択します。

アプリケーション・データのバックアップおよびリストア

`marathon-volume-backup.py` スクリプトを使用して、アプリケーション・データのバックアップおよびリカバリーを行います。

このタスクについて

「バックアップおよびリカバリー」ウィンドウで行う構成バックアップでは、アプリケーションのデータはバックアップされません。`/usr/local/bin/marathon-volume-backup.py` スクリプトは毎晩午前 2:30 に実行され、各インストール済みアプリケーションの `/store` のマウント済みボリュームがバックアップされます。デフォルトでは、データは 7 日間保存されます。

このスクリプトを使用して、以下のタスクを実行します。

- インストール済みアプリケーションのデータを手動でバックアップする。
- システム上のインストール済みアプリケーションのデータ・バックアップをすべてリストする。
- インストール済みアプリケーションのデータをリストアする。
- 保存プロセスを実行して、バックアップの保存期間を設定する。

このスクリプトは、QRadar コンソールおよびアプリケーション・ノード (インストールされている場合) の両方にあります。アプリケーション・ノードが追加されると、データ・バックアップ、データ・リストア、および保存は、QRadar コンソール上で実行されなくなります。アプリケーション・ノード上でスクリプトを使用する必要があります。

手順

1. SSH を使用して、root ユーザーとして QRadar コンソールにログインします。
2. /usr/local/bin/ ディレクトリーに移動します。
   - 以下のコマンドを使用して、アプリケーション・データをバックアップします。
     - すべてのアプリケーションのデータを手動でバックアップするには、以下のコマンドを入力します。

       ```
       ./marathon-volume-backup.py backup -p /qapp
       ```
     - 特定のアプリケーションのデータを手動でバックアップするには、以下のコマンドを入力します。

       ```
       ./marathon-volume-backup.py backup -p /qapp-<app_id>
       ```

       ここで、**<app_id>** は、バックアップするデータを含むアプリケーションの ID です。

     marathon-volume-backup.py スクリプトは毎晩現地時間の午前 2:30 に実行され、すべてのインストール済みアプリケーションがバックアップされます。バックアップ・アーカイブは、/store/backup/marathon フォルダーに保管されます。
   - インストール済みアプリケーションのすべてデータ・バックアップを表示するには、以下のコマンドを入力します。

     ```
     ./marathon-volume-backup.py ls
     ```

     このコマンドは、/store/backup/marathon フォルダーに保管されているすべてのバックアップ・アーカイブを出力します。
   - バックアップ・アーカイブをリストアするには、以下のコマンドを入力します。

     ```
     ./marathon-volume-backup.py restore -i <backup name>
     ```

     バックアップ・アーカイブの名前を検索するには、**ls** コマンドを使用します。
   - デフォルトでは、すべてのバックアップ・アーカイブは 1 週間保存されます。保存プロセスは、毎晩現地時間の午前 2:30 にバックアップとともに実行されます。
     - 保存を手動で実行して、デフォルトの保存期間を使用するには、以下のコマンドを入力します。

       ```
       ./marathon-volume-backup.py retention
       ```
     - **-t** (時間 - デフォルトは 1) スイッチおよび **-p** (期間 - デフォルトは 0) スイッチを追加することで、保存期間を手動で設定することもできます。

       -p スイッチは、3 つの値 (週の場合は 0、日の場合は 1、時間の場合は 2) を受け入れます。

例えば、バックアップの保存期間を 3 週間に設定するには、以下のコマンドを入力します。

```
./marathon-volume-backup.py retention -t 3 -p 0
```

- 夜間タイマーによって使用されている保存時間を変更する場合は、以下の systemd サービス・ファイルにある保存コマンドにフラグを追加します。

  ```
  /etc/systemd/system/framework-apps-data-backup.service
  ```

  例えば、毎晩の保存プロセスによって使用されている保存期間を 5 日間に変更するには、以下の行を見つけます。

  ```
  ExecStart=/usr/local/bin/marathon-volume-backup.py retention
  ```

  これを以下に置き換えます。

  ```
  ExecStart=/usr/local/bin/marathon-volume-backup.py retention -t 5 -p
  1
  ```

  変更内容を保存し、systemd の `systemctl daemon-reload` コマンドを実行して、変更を適用します。

第 13 章 フロー・ソースの管理

「フロー・ソース」ウィンドウを使用して、デプロイメントでフロー・ソースを管理します。

フロー・ソースの追加、編集、有効化、無効化、または削除を実行できます。

関連概念:

『第 13 章 フロー・ソースの管理』
「フロー・ソース」ウィンドウを使用して、デプロイメントでフロー・ソースを管理します。

5 ページの『IBM Security QRadar 製品の機能』
IBM Security QRadar 製品資料では、オフェンス、フロー、アセット、ヒストリカル相関などの機能について説明していますが、すべての QRadar 製品でこれらの機能を利用できるわけではありません。使用する製品によっては、説明されている一部の機能をデプロイメントで使用できない場合があります。各製品の機能を確認して、必要な情報を入手してください。

フロー・ソース

IBM Security QRadar アプライアンスの場合、QRadar SIEM は自動的にアプライアンスで物理ポートのデフォルト・フロー・ソースを追加します。また、QRadar SIEM にはデフォルトの NetFlow フロー・ソースも含まれています。

QRadar SIEM がハードウェアにインストールされている場合、QRadar SIEM はネットワーク・インターフェース・カード (NIC) など、物理デバイスのデフォルト・フロー・ソースを自動的に検出して追加しようとします。また、IBM Security QRadar QFlow Collector を割り当てると、QRadar SIEM にデフォルトの NetFlow フロー・ソースが組み込まれます。

QRadar SIEM を使用して、フロー・ソースを統合できます。

フロー・ソースは、内部または外部のいずれかとして分類されます。

内部フロー・ソース
: ネットワーク・インターフェース・カード (NIC) など、管理対象ホストにインストールされているすべての追加ハードウェアが含まれます。管理対象ホストのハードウェア構成によって、内部フロー・ソースには以下のソースが含まれる場合があります。

  - ネットワーク・インターフェース・カード
  - Napatech インターフェース

外部フロー・ソース
: QRadar QFlow コレクター にフローを送信するすべての外部フロー・ソースが含まれます。 QRadar QFlow コレクター が複数のフロー・ソースを受信する場合は、各フロー・ソースに固有名を割り当てることができます。

同じ QRadar QFlow コレクター で外部フロー・データが受信された場合、それぞれの外部フロー・ソース・データを区別するために固有名が役立ちます。

外部フロー・ソースには以下のソースが含まれる場合があります。

- NetFlow
- IPFIX
- sFlow
- J-Flow
- Packeteer
- Flowlog ファイル

QRadar SIEM は、スプーフィングまたは非スプーフィング方式を使用して、外部フローのソース・データを転送できます。

スプーフィング
: フロー・ソースから受信したインバウンド・データをセカンダリー宛先に再送信します。フロー・ソース・データがセカンダリー宛先に確実に送信されるように、データが受信されるポート (管理ポート) に対して、フロー・ソース構成で「モニター・インターフェース」パラメーターを構成します。特定のインターフェースを使用する場合、QRadar QFlow コレクター はポート 2055 でデフォルトの UDP リスニング・ポートを使用するのではなく、プロミスキャス・モード・キャプチャーを使用してフロー・ソース・データを取得します。結果として、QRadar QFlow コレクター はフロー・ソース・パケットを取得してデータを転送することができます。

非スプーフィング
: 非スプーフィング方式の場合、モニター・インターフェース・パラメーターをフロー・ソース構成で Any として構成します。QRadar QFlow コレクター によってリスニング・ポートが開かれます。これはフロー・ソース・データを受信するためにモニター・ポートとして構成されたポートです。データが処理され、別のフロー・ソース宛先に転送されます。データを送信した元のルーターではなく、フロー・ソース・データの送信元 IP アドレスが QRadar SIEM システムの IP アドレスになります。

NetFlow

NetFlow は、Cisco Systems によって開発された独自のアカウンティング・テクノロジーです。NetFlow は、スイッチまたはルーターを通るトラフィック・フローをモニターし、クライアント、サーバー、プロトコル、および使用されるポートを解釈して、バイトおよびパケット数をカウントし、そのデータを NetFlow コレクターに送信します。

NetFlow からデータを送信するプロセスは、NetFlow Data Export (NDE) と呼ばれることがよくあります。NDE を受け入れて、NetFlow コレクターになるように IBM Security QRadar を構成できます。QRadar は、NetFlow バージョン 1、5、7、および 9 をサポートしています。NetFlow について詳しくは、Cisco Web サイト (http://www.cisco.com) を参照してください。

NetFlow ではモニターされるネットワークの量が拡大されますが、無接続プロトコル (UDP) を使用して NDE が送信されます。スイッチまたはルーターから NDE が送信された後、NetFlow レコードはパージされます。この情報の送信には UDP が使用され、データの送信が保証されないため、NetFlow の記録は不正確になり、アラート機能は低下します。これにより、トラフィック量と双方向フローの両方の表示が不正確になる可能性があります。

NetFlow 用に外部フロー・ソースを構成するときは、以下のタスクを実行する必要があります。

- 適切なファイアウォール・ルールが構成されていることを確認します。IBM Security QRadar QFlow Collector 構成で外部フロー・ソース・モニター・ポートのパラメーターを変更する場合、ファイアウォール・アクセス構成も更新する必要があります。
- QRadar QFlow コレクター に対して適切なポートが構成されていることを確認します。

NetFlow バージョン 9 を使用している場合、NetFlow ソースの NetFlow テンプレートに以下のフィールドが含まれていることを確認します。

- FIRST_SWITCHED
- LAST_SWITCHED
- PROTOCOL
- IPV4_SRC_ADDR
- IPV4_DST_ADDR
- L4_SRC_PORT
- L4_DST_PORT
- IN_BYTES または OUT_BYTES
- IN_PKTS または OUT_PKTS
- TCP_FLAGS (TCP フローのみ)

IPFIX

Internet Protocol Flow Information Export (IPFIX) はアカウンティング・テクノロジーです。IPFIX は、スイッチまたはルーターを通るトラフィック・フローをモニターし、クライアント、サーバー、プロトコル、および使用されるポートを解釈して、バイト数およびパケット数をカウントし、そのデータを IPFIX コレクターに送信します。

次世代の侵入防止システム (IPS) である IBM Security Network Protection XGS 5000 は、IPFIX フロー・フォーマットでフロー・トラフィックを送信するデバイスの一例です。

IPFIX データを送信するプロセスは、NetFlow Data Export (NDE) と呼ばれることがよくあります。IPFIX は、NetFlow v9 よりも多くのフロー情報とより深い洞察を提供します。NDE を受け入れて、IPFIX コレクターになるように IBM Security QRadar を構成できます。IPFIX はユーザー・データグラム・プロトコル (UDP) を使用して NDE を送信します。IPFIX 転送デバイスから NDE が送信された後、IPFIX レコードはパージされる場合があります。

IPFIX フロー・トラフィックを受け入れるように QRadar を構成するには、NetFlow フロー・ソースを追加する必要があります。NetFlow フロー・ソースは同じプロセスを使用して IPFIX フローを処理します。

ご使用の QRadar システムにデフォルトの NetFlow フロー・ソースが含まれている可能性があります。このため、NetFlow フロー・ソースを構成する必要がない場合があります。システムにデフォルトの NetFlow フロー・ソースが含まれていることを確認するには、「管理」 > 「フロー・ソース」を選択します。**default_Netflow** がフロー・ソース・リストにリストされている場合、IPFIX は既に構成されています。

IPFIX 用に外部フロー・ソースを構成するときは、以下のタスクを実行する必要があります。

- 適切なファイアウォール・ルールが構成されていることを確認します。IBM Security QRadar QFlow Collector 構成で外部フロー・ソース・モニター・ポートのパラメーターを変更する場合、ファイアウォール・アクセス構成も更新する必要があります。QRadar QFlow コレクター 構成について詳しくは、「*IBM Security QRadar* 管理ガイド」を参照してください。
- QRadar QFlow コレクター に対して適切なポートが構成されていることを確認します。
- IPFIX ソースの IPFIX テンプレートに以下のフィールドが含まれていることを確認します。
- FIRST_SWITCHED
- LAST_SWITCHED
- PROTOCOL
- IPV4_SRC_ADDR
- IPV4_DST_ADDR
- L4_SRC_PORT
- L4_DST_PORT
- IN_BYTES または OUT_BYTES
- IN_PKTS または OUT_PKTS
- TCP_FLAGS (TCP フローのみ)

sFlow

sFlow は、すべてのインターフェース上のアプリケーション・レベルのトラフィック・フローを同時かつ継続的にモニターするサンプリング技術のための複数ベンダーとユーザーの標準です。

sFlow は、インターフェース・カウンターとフロー・サンプルを sFlow データグラムに結合します。このデータグラムは、sFlow コレクターに対するネットワーク全体に送信されます。IBM Security QRadar は、sFlow バージョン 2、4、5 をサポートしています。sFlow トラフィックはサンプル・データを基にしているため、必ずしもすべてのネットワーク・トラフィックを表しているとは限りません。詳しくは、sFlow の Web サイト (www.sflow.org) を参照してください。

sFlow では無接続プロトコル (UDP) が使用されます。スイッチまたはルーターからデータが送信されると、sFlow レコードはパージされます。この情報の送信には UDP が使用され、データの送信が保証されないため、sFlow の記録は不正確になり、アラート機能は低下します。これにより、トラフィック量と双方向フローの両方の表示が不正確になる可能性があります。

sFlow 用に外部フロー・ソースを構成するときは、以下のタスクを実行する必要があります。

- 適切なファイアウォール・ルールが構成されていることを確認します。
- QRadar VFlow コレクター に対して適切なポートが構成されていることを確認します。

J-Flow

IP トラフィック・フロー統計を収集できる Juniper Networks によって使用される独自のアカウンティング・テクノロジーです。J-Flow を使用して、データを J-Flow コレクター上の UDP ポートにエクスポートできます。J-Flow を使用して、ルーターまたはインターフェースで J-Flow を有効にし、ネットワークの特定の場所に関するネットワーク統計を収集することもできます。

J-Flow トラフィックはサンプル・データに基づいているため、一部のネットワーク・トラフィックが示されない可能性があることに注意してください。J-Flow について詳しくは、Juniper Networks Web サイト (www.juniper.net) を参照してください。

J-Flow では無接続プロトコル (UDP) が使用されます。スイッチまたはルーターからデータが送信されると、J-Flow レコードはパージされます。この情報の送信には UDP が使用され、データの送信が保証されないため、J-Flow の記録は不正確になり、アラート機能は低下します。これにより、トラフィック量と双方向フローの両方の表示が不正確になる可能性があります。

J-Flow 用に外部フロー・ソースを構成するときは、以下を行う必要があります。

- 適切なファイアウォール・ルールが構成されていることを確認します。
- IBM Security QRadar QFlow Collector に対して適切なポートが構成されていることを確認します。

Packeteer

Packeteer デバイスは、ネットワーク・パフォーマンス・データを収集、集約、および保存します。Packeteer の外部フロー・ソースを構成した後、Packeteer デバイスから IBM Security QRadar にフロー情報を送信できます。

Packeteer では無接続プロトコル (UDP) が使用されます。スイッチまたはルーターからデータが送信されると、Packeteer レコードはパージされます。この情報の送信には UDP が使用され、データの送信が保証されないため、Packeteer の記録は不正確になり、アラート機能は低下します。トラフィック量と双方向フローの両方の表示が不正確になる可能性があります。

外部フロー・ソースとして Packeteer を構成するには、以下のタスクを実行する必要があります。

- 適切なファイアウォール・ルールが構成されていることを確認します。
- フローの詳細レコードをエクスポートするように Packeteer デバイスを構成し、データのエクスポート先として IBM Security QRadar QFlow Collector を構成していることを確認します。
- QRadar QFlow コレクター に対して適切なポートが構成されていることを確認します。
- Packeteer デバイスからのクラス ID が QRadar QFlow コレクター によって自動的に検出されることを確認します。
- 詳しくは、「*Mapping Packeteer Applications into QRadar Technical Note*」を参照してください。

Flowlog ファイル

Flowlog ファイルは、IBM Security QRadar フロー・ログから生成されます。

Napatech インターフェース

Napatech ネットワーク・アダプターを IBM Security QRadar システムにインストールしてある場合、「**Napatech** インターフェース」オプションが QRadar ユーザー・インターフェースに構成可能なパケット・ベースのフロー・ソースとして表示されます。 Napatech ネットワーク・アダプターには、使用するネットワークに合わせてプログラム可能な次世代インテリジェント・ネットワーク・アダプターが備わっています。詳しくは、Napatech の資料を参照してください。

フロー・ソースの追加または編集

「フロー・ソース (Flow Source)」ウィンドウを使用して、フロー・ソースを追加します。

手順

1. 「管理」タブをクリックします。
2. ナビゲーション・メニューで、「データ・ソース」をクリックします。
3. ナビゲーション・メニューで、「フロー」をクリックします。
4. 「フロー・ソース」をクリックします。
5. 以下のいずれかのアクションを実行します。
   - フロー・ソースを追加するには、「追加 **(Add)**」をクリックします。
   - フロー・ソースを編集するには、対象のフロー・ソースを選択して「編集」をクリックします。
6. 既存のフロー・ソースを使用して新しいフロー・ソースを作成するには、「既存のフロー・ソースから作成」チェック・ボックスを選択してから、「テンプレートとして使用」リストで任意のフロー・ソースを選択します。
7. 「フロー・ソース名」に名前を入力します。

   ヒント**:** 外部フロー・ソースが物理デバイスでもある場合は、そのデバイス名をフロー・ソース名として使用してください。フロー・ソースが物理デバイスではない場合は、わかりやすい名前を入力してください。

例えば、IPFIX トラフィックを使用する場合は「**ipf1**」と入力します。NetFlow トラフィックを使用する場合は、「**nf1**」と入力します。

8. 「フロー・ソース・タイプ」リストでフロー・ソースを選択し、各プロパティーを設定します。
   - 「**Flowlog** ファイル」オプションを選択した場合は、「ソース・ファイル・パス」パラメーターで Flowlog ファイルの場所を設定する必要があります。
   - 「フロー・ソース・タイプ」パラメーターで「**JFlow**」、「**Netflow**」、「**Packeteer**」、「**FDR**」、「**sFlow**」のいずれかのオプションを選択した場合は、使用可能なポートを「モニター・ポート」パラメーターで設定する必要があります。

     ネットワーク内で構成されている NetFlow の最初のフロー・ソースのデフォルト・ポートは 2055 です。NetFlow のその他の各フロー・ソースについては、デフォルトのポート番号が 1 ずつ増えていきます。例えば、NetFlow の 2 番目のフロー・ソースのデフォルト・ポートは 2056 になります。
   - 「**Napatech** インターフェース」オプションを選択した場合は、フロー・ソースに割り当てたいフロー・インターフェースを入力する必要があります。

     制約事項: 「**Napatech** インターフェース」オプションは、Napatech ネットワーク・アダプターがシステムにインストールされている場合のみ表示されます。
   - 「フロー・インターフェース」で「ネットワーク・インターフェース」オプションを選択した場合は、各イーサネット・インターフェースについてログ・ソースを 1 つだけ設定してください。

     制約事項: 同じポートに異なるフロー・タイプを送信することはできません。
9. ネットワーク上のトラフィックが、インバウンド・トラフィックとアウトバウンド・トラフィックについて代替パスを使用するように構成されている場合は、「非対称フローを使用可能にする」チェック・ボックスを選択します。
10. 「保存」をクリックします。
11. 「管理」タブ・メニューで、「変更のデプロイ」をクリックします。

QRadar Packet Capture へのパケットの転送

生データ・パケットを IBM Security QRadar QFlow Collector 1310 アプライアンスに送信することにより、ネットワーク・トラフィックをモニターできます。QRadar QFlow コレクター は、専用の Napatech モニタリング・カードを使用して、着信パケットをカード上のあるポートから IBM Security QRadar Packet Capture アプライアンスに接続する別のポートへとコピーします。

10G Napatech ネットワーク・カードを備えた QRadar QFlow コレクター 1310 が既にある場合、トラフィックを QRadar Packet Capture にミラーリングできます。

次の図に示すように、10G Napatech ネットワーク・カードを備えた QRadar QFlow コレクター 1310 が既にある場合、トラフィックを QRadar Packet Capture にミラーリングできます。

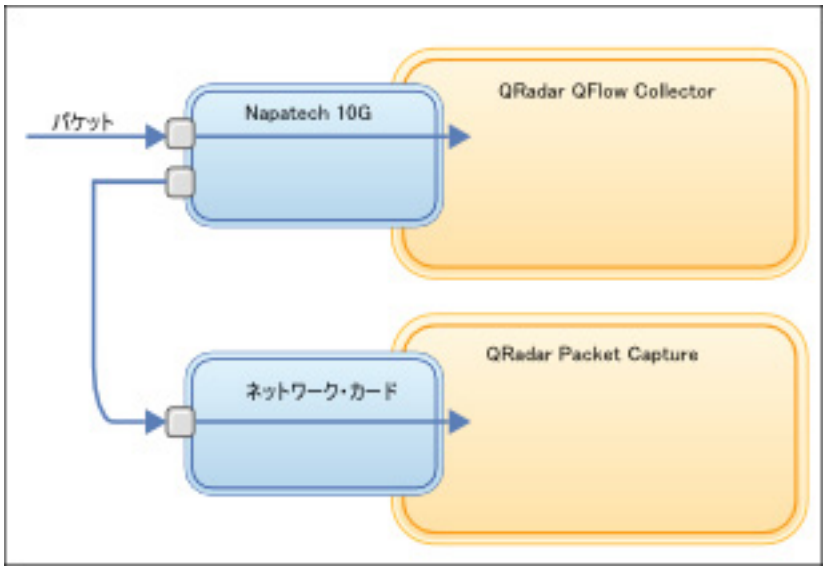


図 *9. Napatech* カードを使用して *QRadar QFlow* コレクター から *QRadar Packet Capture* に転送されるパケット・データ

始める前に

以下のハードウェアがご使用の環境にセットアップされていることを確認してください。

- QRadar QFlow コレクター 1310 アプライアンスの Napatech カードのポート 1 にケーブルを接続している。
- Napatech カードのポート 2 (転送ポート) に接続されているケーブルを QRadar Packet Capture アプライアンスに接続している。
- 両方のアプライアンスでリンク・ライトを確認してレイヤー 2 接続を検証します。

手順

1. IBM Security QRadar コンソールから、SSH を使用して root ユーザーとして QRadar QFlow コレクター にログインします。QRadar QFlow コレクター アプライアンスで、以下のファイルを編集します。

   ```
   /opt/qradar/init/apply_tunings
   ```

   a. 137 行目あたりにある、以下の行を見つけます。

   ```
   apply_multithread_qflow_changes()
   {
        APPLIANCEID=`$NVABIN/myver -a`
        if [ "$APPLIANCEID" == "1310" ]; then
             MODELNUM=$(/opt/napatech/bin/AdapterInfo 2>&1 | grep "Active FPGA Image" | cut -d'-' -f2)
             if [ "$MODELNUM" == "9220" ]; then..
   ```

   b. 上記のコードに続く一連の AppendToConf の行に、次の行を追加します。

   ```
   AppendToConf SV_NAPATECH_FORWARD YES
   AppendToConf SV_NAPATECH_FORWARD_INTERFACE_SRCDST "0:1"
   ```

これらのステートメントにより、パケット転送が有効になり、パケットがポート 0 からポート 1 に転送されます。

c. /opt/qradar/conf/nva.conf ファイルの以下の行を確認してマルチスレッド化 が有効になっていることを検証します。

```
MULTI_THREAD_ON=YES
```

2. 以下のコマンドを入力して apply_tunings スクリプトを実行し、QRadar QFlow コレクター の構成ファイルを更新します。

```
./apply_tunings restart
```

3. 以下のコマンドを入力して IBM Security QRadar サービスを再始動します。

```
systemctl restart hostcontext
```

4. オプション: Napatech カードがデータを送受信しているか確認します。

a. Napatech カードがデータを受信しているか確認するには、以下のコマンドを入力します。

```
/opt/napatech/bin/Statistics -dec -interactive
```

カードがデータを受信している場合、「RX」パケットとバイトの統計が増加します。

b. Napatech カードがデータを送信しているか確認するには、以下のコマンドを入力します。

```
/opt/napatech/bin/Statistics -dec -interactive
```

カードがデータを送信している場合、「TX」統計が増加します。

5. オプション: QRadar Packet Capture が QRadar QFlow コレクター アプライアンスからパケットを受信していることを検証します。

a. QRadar コンソールから、SSH を使用して root ユーザーとしてポート 4477 で QRadar Packet Capture アプライアンスにログインします。

b. 以下のコマンドを入力して、QRadar Packet Capture アプライアンスがパケットを受信していることを検証します。

```
watch -d cat /var/www/html/statisdata/int0.txt
```

データが QRadar Packet Capture アプライアンスに送信されるたびに int0.txt ファイルが更新されます。

パケット・キャプチャーについて詳しくは、「*IBM Security QRadar Packet Capture* クイック・リファレンス・ガイド」を参照してください。

フロー・ソースの有効化および無効化

「フロー・ソース (Flow Source)」ウィンドウを使用して、フロー・ソースを有効または無効に設定できます。

手順

1. 「管理」タブをクリックします。
2. ナビゲーション・メニューで、「データ・ソース」をクリックします。
3. ナビゲーション・メニューで、「フロー」をクリックします。
4. 「フロー・ソース」アイコンをクリックします。
5. 有効または無効にするフロー・ソースを選択します。

   「有効」列は、フロー・ソースが有効か無効かどうかを示します。

   以下の状況が表示されます。

   - True は、フロー・ソースが有効であることを示します。
   - False は、フロー・ソースが現在無効であることを示します。
6. 「有効/無効」をクリックします。
7. 「管理」タブ・メニューで、「変更のデプロイ」をクリックします。

フロー・ソースの削除

「フロー・ソース (Flow Source)」ウィンドウを使用して、フロー・ソースを削除します。

手順

1. 「管理」タブをクリックします。
2. ナビゲーション・メニューで、「データ・ソース」をクリックします。
3. ナビゲーション・メニューで、「フロー」をクリックします。
4. 「フロー・ソース」をクリックします。
5. 削除するフロー・ソースを選択します。
6. 「削除」をクリックします。
7. 「**OK**」をクリックします。
8. 「管理」タブ・メニューで、「変更のデプロイ」をクリックします。

フロー・ソースの別名の管理

「フロー・ソースの別名」ウィンドウを使用して、フロー・ソースの仮想名、または別名を構成します。

送信元 IP アドレスと仮想名を使用して、同じ IBM Security QRadar QFlow Collector に送信される複数のソースを特定します。別名により、QRadar QFlow コレクター は同じポートに送信されるデータ・ソースを一意に識別し、処理することができます。

QRadar QFlow コレクター が、IP アドレスは持つが現在の別名を持たないデバイスからトラフィックを受け取ると、QRadar QFlow コレクター は、リバース DNS ルックアップを試行します。このルックアップは、デバイスのホスト名を決定するために使用されます。ルックアップが成功すると、QRadar QFlow コレクター はこの情報をデータベースに追加し、デプロイメント内のすべての QRadar QFlow コレクター コンポーネントにこの情報をレポートします。

「管理」タブの「システムおよびライセンス管理」を使用して、QRadar QFlow コレクターが自動的にフロー・ソースの別名を検出するように構成します。

フロー・ソース別名の追加

「フロー・ソースの別名」ウィンドウを使用して、フロー・ソース別名を追加します。

手順

1. 「管理」タブをクリックします。
2. ナビゲーション・メニューで、「データ・ソース」をクリックします。
3. ナビゲーション・メニューで、「フロー」をクリックします。
4. 「フロー・ソースの別名 **(Flow Source Aliases)**」アイコンをクリックします。
5. 以下のいずれかのアクションを実行します。
   - フロー・ソースの別名を追加するには、「追加」をクリックして、各パラメーターの値を入力します。
   - 既存のフロー・ソースの別名を編集するには、対象のフロー・ソースの別名を選択して「編集」をクリックし、パラメーターを更新します。
6. 「保存」をクリックします。
7. 「管理」タブ・メニューで、「変更のデプロイ」をクリックします。

フロー・ソース別名の削除

「フロー・ソースの別名」ウィンドウを使用して、フロー・ソース別名を削除します。

手順

1. 「管理」タブをクリックします。
2. ナビゲーション・メニューで、「データ・ソース」をクリックします。
3. ナビゲーション・メニューで、「フロー」をクリックします。
4. 「フロー・ソースの別名 **(Flow Source Aliases)**」アイコンをクリックします。
5. 削除するフロー・ソース別名を選択します。
6. 「削除」をクリックします。
7. 「**OK**」をクリックします。
8. 「管理」タブ・メニューで、「変更のデプロイ」をクリックします。

第 14 章 リモート・ネットワークおよびサービスの構成

リモート・ネットワーク・グループとサービス・グループを使用して、ネットワーク上の特定のプロファイル用のトラフィック・アクティビティーを表します。リモート・ネットワーク・グループには、指定されたリモート・ネットワークから発生するユーザー・トラフィックが表示されます。

すべてのリモート・ネットワーク・グループとサービス・グループには、グループ・レベルとリーフ・オブジェクト・レベルがあります。既存のグループにオブジェクトを追加するか、既存のプロパティーを変更することにより、リモート・ネットワーク・グループとサービス・グループを編集し、環境に適合させることができます。

既存のオブジェクトを別のグループに移動すると、オブジェクト名が既存のグループから新しく選択したグループに移動します。ただし、構成の変更がデプロイされると、データベースに保管されているオブジェクト・データが失われるため、そのオブジェクトは機能しなくなります。この問題を解決するには、新しいビューを作成して、別のグループに存在するオブジェクトを再作成します。

カスタム・ルール・エンジン、フロー検索、およびイベント検索で使用するために、「管理」タブでリモート・ネットワークとサービスをグループ化することができます。使用可能な場合は、IBM Security QRadar Risk Manager でも、ネットワークとサービスをグループ化することができます。

関連概念:

5 ページの『IBM Security QRadar 製品の機能』
IBM Security QRadar 製品資料では、オフェンス、フロー、アセット、ヒストリカル相関などの機能について説明していますが、すべての QRadar 製品でこれらの機能を利用できるわけではありません。使用する製品によっては、説明されている一部の機能をデプロイメントで使用できない場合があります。各製品の機能を確認して、必要な情報を入手してください。

デフォルトのリモート・ネットワーク・グループ

IBM Security QRadar には、デフォルトのリモート・ネットワーク・グループが含まれています。

以下の表で、デフォルトのリモート・ネットワーク・グループについて説明します。

表 48. デフォルトのリモート・ネットワーク・グループ

グループ	説明
BOT	BOT アプリケーションから発生するトラフィックを指定します。 詳しくは、Emerging Threats Web サイトの Botnet Command and Control drop rules (http://rules.emergingthreats.net/blockrules/emerging-botcc.rules) を参照してください。
Bogon	未割り当ての IP アドレスから発生するトラフィックを指定します。 詳しくは、Team CYMRU Web サイトの bogon に関するリファレンス (http://www.team-cymru.org/Services/Bogons/bogon-bn-nonagg.txt) を参照してください。
HostileNets	悪意のある既知のネットワークから発生するトラフィックを指定します。 HostileNets には、20 (ランク 1 から 20 まで) の構成可能な CIDR 範囲があります。 詳しくは、DShield Web サイトの HostileNets に関するリファレンス (http://www.dshield.org/ipsascii.html?limit=20) を参照してください。
Neighbours	組織がネットワーク・ピアリング契約を結んでいる近隣ネットワークから発生するトラフィックを指定します。 このグループは、デフォルトでブランクになっています。近隣ネットワークから発生するトラフィックを分類するには、このグループを構成する必要があります。
Smurfs	スマーフ攻撃から発生するトラフィックを指定します。 スマーフ攻撃は、スプーフされたブロードキャスト ping メッセージで宛先システムをあふれさせるサービス拒否攻撃の一種です。
Superflows	このグループを構成することはできません。 スーパーフローは、類似する一連の事前定義エレメントを持つ多数のフローを集約したフローです。

表 48. デフォルトのリモート・ネットワーク・グループ (続き)

グループ	説明
TrustedNetworks	トラステッド・ネットワーク (重要なアプリケーションおよびサービスに対するリモート・アクセス権限を持つビジネス・パートナーを含む) からのトラフィックを指定します。 このグループは、デフォルトでブランクになっています。 トラステッド・ネットワークから発生するトラフィックを分類するには、このグループを構成する必要があります。
Watchlists	モニター対象のネットワークから発生するトラフィックを分類します。 このグループは、デフォルトでブランクになっています。

スーパーフローを持つグループとオブジェクトは、情報提供だけを目的としているため、編集することはできません。bogon を持つグループとオブジェクトは、自動更新機能によって構成されます。

注: リモート・ネットワークの代わりにリファレンス・セットを使用して、この機能の一部を実行することができます。リファレンス・テーブルで IP 値に信頼度レベルを割り当てることはできますが、リファレンス・セットは単一 IP でのみ使用され、CIDR 範囲では使用できません。リモート・ネットワークの更新後に CIDR 値を使用できますが、重みレベルや信頼度レベルとともに使用することはできません。

関連概念:

170 ページの『リファレンス・データ収集のタイプ』
さまざまなタイプのリファレンス・データ収集が存在し、それぞれのタイプは、異なるレベルの複雑さのデータを扱うことができます。最も一般的なタイプはリファレンス・セットとリファレンス・マップです。

デフォルトのリモート・サービス・グループ

IBM Security QRadar には、デフォルトのリモート・サービス・グループが含まれます。

以下の表で、デフォルトのリモート・サービス・グループについて説明します。

表 49. デフォルトのリモート・ネットワーク・グループ

パラメーター	説明
IRC_Servers	チャット・サーバーとして一般的に知られているアドレスからのトラフィックを指定します。

表 49. デフォルトのリモート・ネットワーク・グループ (続き)

パラメーター	説明
Online_Services	データ損失が発生する可能性のあるオンライン・サービスとして一般的に知られているアドレスからのトラフィックを指定します。
Porn	露骨なポルノ素材が存在することが一般的に知られているアドレスからのトラフィックを指定します。
Proxies	一般的に知られている公開プロキシー・サーバーからのトラフィックを指定します。
Reserved_IP_ Ranges	予約済み IP アドレス範囲からのトラフィックを指定します。
Spam	スパムや不要な E メールを生成することが一般的に知られているアドレスからのトラフィックを指定します。
Spy_Adware	スパイウェアまたはアドウェアが存在することが一般的に知られているアドレスからのトラフィックを指定します。
Superflows	スーパーフローを生成することが一般的に知られているアドレスからのトラフィックを指定します。
Warez	海賊版ソフトウェアが存在することが一般的に知られているアドレスからのトラフィックを指定します。

ネットワーク・リソースのガイドライン

大規模な構造のネットワークにおいて、IBM Security QRadar SIEM が必要とする複雑性やネットワーク・リソースを考慮し、推奨ガイドラインに従ってください。

以下のリストで、推奨されるプラクティスの一部を説明します。

- オブジェクトをバンドルし、「ネットワーク・アクティビティー」タブと「ログ・アクティビティー」タブを使用して、ネットワーク・データを分析してください。

  オブジェクトの数を減らすと、ディスクに対する入出力が少なくなります。
- 通常、標準的なシステム要件の場合、グループ当たりのオブジェクト数は 200 以内にしてください。

  オブジェクト数がこれよりも多くなると、トラフィックを調査する際の処理能力に影響する可能性があります。

リモート・ネットワーク・オブジェクトの管理

リモート・ネットワーク・グループを作成すると、リモート・ネットワーク・グループのフローとイベントの検索結果を集約できるようになります。また、リモート・ネットワーク・グループのアクティビティーをテストするためのルールを作成できるようにもなります。

「リモート・ネットワーク」ウィンドウを使用して、リモート・ネットワーク・オブジェクトを追加または編集することができます。

手順

1. 「管理」タブをクリックします。
2. ナビゲーション・メニューで、「リモート・ネットワークおよびサービス構成 **(Remote Networks and Services Configuration)**」をクリックします。
3. 「リモート・ネットワーク」アイコンをクリックします。
4. リモート・ネットワーク・オブジェクトを追加するには、「追加」をクリックしてパラメーターの値を入力します。
5. リモート・ネットワーク・オブジェクトを編集するには、表示するグループをクリックし、「編集」をクリックしてから値を変更します。
6. 「保存」をクリックします。
7. 「戻る」をクリックします。
8. 「リモート・ネットワーク」ウィンドウを閉じます。
9. 「管理」タブ・メニューで、「変更のデプロイ」をクリックします。

リモート・サービス・オブジェクトの管理

リモート・サービス・グループは、ユーザー定義のネットワーク範囲または IBM 自動更新サーバーから発生するトラフィックを編成します。リモート・サービス・グループを作成すると、リモート・サービス・グループのフローとイベントの検索結果を集約したり、リモート・サービス・グループのアクティビティーをテストするためのルールを作成したりできるようになります。

「リモート・サービス」ウィンドウを使用して、リモート・サービス・オブジェクトを追加または編集します。

手順

1. 「管理」タブをクリックします。
2. ナビゲーション・メニューで、「リモート・ネットワークおよびサービス構成 **(Remote Networks and Services Configuration)**」をクリックします。
3. 「リモート・サービス」アイコンをクリックします。
4. リモート・サービス・オブジェクトを追加するには、「追加」をクリックしてパラメーター値を入力します。
5. リモート・サービス・オブジェクトを編集するには、表示するグループをクリックし、「編集」アイコンをクリックして値を変更します。
6. 「保存」をクリックします。
7. 「戻る」をクリックします。

8. 「リモート・サービス」ウィンドウを閉じます。
9. 「管理」タブ・メニューで、「変更のデプロイ」をクリックします。

QID マップの概要

IBM Security QRadar Identifier (QID) マップ・ユーティリティーを使用して、ユーザー定義の QID マップ・エントリーを作成、エクスポート、インポート、または変更します。

QID マップは、外部デバイス上のイベントを QID に関連付けます。

QID の管理については、以下のタスクを参照してください。

- 『QID マップ・エントリーの作成』
- 247 ページの『QID マップ・エントリーの変更』
- 248 ページの『Qid マップ・エントリーのインポート』
- 249 ページの『QID マップ・エントリーのエクスポート』

ユーティリティーを実行するには、以下の構文を使用します。

```
qidmap_cli.sh [-l|-c|-m|-i[-f <filename>]|-e[-f <filename>]|-d]
```

以下の表で、QID マップ・ユーティリティーのコマンド行オプションについて説明します。

表 *50. QID* マップ・ユーティリティーのオプション

オプション	説明
-l	下位カテゴリーをリストします。
-c	QID マップ・エントリーを作成します。
-m	既存のユーザー定義の QID マップ・エントリーを変更します。
-i	QID マップ・エントリーをインポートします。
-e	既存のユーザー定義の QID マップ・エントリーをエクスポートします。
-f <filename>	-i または -e オプションを使用する場合に、QID マップ・エントリーをインポートまたはエクスポートするファイルの名前を指定します。
-d	-i または -e オプションを使用する場合に、インポート・ファイルまたはエクスポート・ファイルの区切り文字を指定します。デフォルトはコンマです。
-h	ヘルプ・オプションを表示します。

QID マップ・エントリーの作成

外部デバイスのイベントを QID にマップするには、IBM Security QRadar Identifier (QID) マップ・エントリーを作成します。

手順

1. SSH を使用して、root ユーザーとして QRadar にログインします。

2. 作成する QID マップ・エントリーの下位カテゴリーを見つけるために、次のコマンドを入力します。

   ```
   /opt/qradar/bin/qidmap_cli.sh -l
   ```

   特定の下位カテゴリーを検索する場合は、次のように grep コマンドを使用して、結果をフィルターに掛けます。

   ```
   /opt/qradar/bin/qidmap_cli.sh -l | grep <text>
   ```

3. 以下のコマンドを入力します。

   ```
   qidmap_cli.sh -c --qname <name> --qdescription <description>
   --severity <severity> --lowlevelcategoryid <ID>
   ```

   以下の表で、QID マップ・ユーティリティーのコマンド行オプションについて説明します。

オプション	説明
-c	QID マップ・エントリーを作成する。
--qname <*name*>	この QID マップ・エントリーに関連付ける名前。名前の長さは 255 文字まで可能です。 名前にスペースを含める場合は、名前の値を二重引用符で囲んでください。
--qdescription <*description*>	この QID マップ・エントリーの説明。説明の長さは最大で 2048 文字までです。 説明にスペースを含める場合は、説明の値を二重引用符で囲んでください。
--severity <*severity*>	この QID マップ・エントリーに割り当てる重大度レベル。有効な範囲は 1 から 10 です。
--lowlevelcategoryid <*ID*>	この QID マップ・エントリーに割り当てる下位カテゴリーの ID。詳しくは、「*IBM Security QRadar* 管理ガイド」を参照してください。

QID マップ・エントリーの変更

既存のユーザー定義の IBM Security QRadar Identifier (QID) マップ・エントリーを変更します。

手順

1. SSH を使用して、root ユーザーとして QRadar にログインします。
2. 以下のコマンドを入力します。

   ```
   qidmap_cli.sh -m --qid<QID> --qname <name> --qdescription <description>
   --severity <severity>
   ```

   以下の表で、QID マップ・ユーティリティーのコマンド行オプションについて説明します。

オプション	説明
-m	既存のユーザー定義の QID マップ・エントリーを変更します。
--qid<*QID*>	変更する QID。
--qname <*name*>	この QID マップ・エントリーに関連付ける名前。名前の最大長は 255 文字で、スペースは使用しません。
--qdescription <*description*>	この QID マップ・エントリーの説明。説明の最大長は 2048 文字で、スペースは使用しません。
--severity <*severity*>	この QID マップ・エントリーに割り当てる重大度レベル。有効な範囲は 0 から 10 です。

Qid マップ・エントリーのインポート

IBM Security QRadar Identifier (QID) マップ・ユーティリティーを使用して、.txt ファイルから QID マップ・エントリーをインポートすることができます。

手順

1. インポートするユーザー定義の QID マップ・エントリーを含む .txt ファイルを作成します。ファイル内の各エントリーがコンマで区切られるようにします。次のオプションのいずれかを選択してください。
   - ユーザー定義の QID マップ・エントリーの新規リストをインポートする場合は、各エントリーで次の形式を使用してファイルを作成します。

     ```
     ,<name>,<description>,<severity>,<category>
     ```

     例:

     ```
     ,buffer,buffer_QID,7,18401 ,malware,malware_misc,8,18403
     ```
   - ユーザー定義の QID マップ・エントリーの既存のリストをインポートする場合は、各エントリーで次の形式を使用してファイルを作成します。

     ```
     <qid>,<name>,<description>,<severity>
     ```

     例: `2000002,buffer,buffer_QID,7 2000001,malware,malware_misc`

   以下の表で、QID ユーティリティーのコマンド行オプションについて説明します。

オプション	説明
<*qid*>	エントリーの既存の QID。このオプションは、エクスポートされた既存の QID エントリーのリストをインポートする場合に必要です。 新規の QID エントリーをインポートする場合は、このオプションを使用しないでください。QID マップ・ユーティリティーは、ファイル内のエントリーごとに ID (QID) を割り当てます。
--qname <*name*>	この QID マップ・エントリーに関連付ける名前。名前の最大長は 255 文字で、スペースは使用しません。
--qdescription <*description*>	この QID マップ・エントリーの説明。説明の最大長は 2048 文字で、スペースは使用しません。
--severity <*severity*>	この QID マップ・エントリーに割り当てる重大度レベル。有効な範囲は 0 から 10 です。
--lowlevelcategoryid <*ID*>	この QID マップ・エントリーに割り当てる下位カテゴリーの ID。 このオプションは、新規の QID エントリーのリストをインポートする場合にのみ必要です。

2. ファイルを保存して閉じます。
3. SSH を使用して、root ユーザーとして QRadar にログインします。
4. QID マップ・ファイルをインポートするには、以下のコマンドを入力します。

```
/opt/qradar/bin/qidmap_cli.sh -i -f
<filename.txt>
```

<*filename.txt*> オプションは、QID マップ・エントリーが含まれているファイルのディレクトリー・パスおよびファイル名です。ファイル内のいずれかのエントリーでエラーが発生した場合、ファイル内のどのエントリーも適用されません。

QID マップ・エントリーのエクスポート

QID エントリーをエクスポートすることにより、外部デバイスのイベントとその固有 ID との間のマッピングを表示します。

このタスクについて

作成した QID マップ・エントリーの場合は、QID マップ・ユーティリティーを使用して、エントリーを .txt ファイルにエクスポートします。

デフォルトのシステム QID エントリーを含む QID マップ全体の場合は、**idlist.sh** コマンドを使用します。

手順

1. SSH を使用して、root ユーザーとして IBM Security QRadar にログインします。
2. ユーザー定義エントリーの QID マップ・ファイルをエクスポートするには、以下のコマンドを入力します。

   ```
   /opt/qradar/bin/qidmap_cli.sh -e -f
   <filename.txt>
   ```

   <filename.txt> オプションは、QID マップ・エントリーを格納するファイルのディレクトリー・パスおよびファイル名です。
3. QID マップ全体をエクスポートするには、以下のコマンドを入力します。

   ```
   /opt/qradar/bin/idlist.sh -e qid > <filename.txt>
   ```
4. QID マップの最終変更日を判別するために、SQL 照会を実行します。 例えば、QID の ID 番号が 64250088 の場合、以下の SQL 照会を入力して最終変更日を取得します。

   ```
   psql -U qradar -c "select qid,to_timestamp(serial/1000) as date from
   qidmap_serial where qid = 64250088;"
   ```

第 15 章 サーバー・ディスカバリー

サーバー・ディスカバリー機能は、アセット・プロファイル・データベースを使用して、ポート定義に基づく各種サーバー・タイプをディスカバーします。ディスカバーされたサーバーを選択して、ルール用のサーバー・タイプのビルディング・ブロックに追加することができます。

サーバー・ディスカバリー機能は、サーバー・タイプのビルディング・ブロックに基づいています。ポートを使用して、サーバー・タイプが定義されます。そのため、サーバー・タイプのビルディング・ブロックは、アセット・プロファイル・データベースを検索する際に、ポート・ベースのフィルターとして機能します。

ビルディング・ブロックについて詳しくは、「*IBM Security QRadar* ユーザー・ガイド」を参照してください。

IBM Security QRadar Vulnerability Manager の「サーバー・ディスカバリー」機能を使用して、良性の脆弱性用の例外ルールを作成します。以下のサーバー・タイプについて表示される脆弱性の数を減らしてください。

表 *51.* サーバー・タイプの脆弱性

サーバー・タイプ	脆弱性
FTP サーバー	**FTP** サーバーが存在します
DNS サーバー	**DNS** サーバーが稼働しています
メール・サーバー	**SMTP** サーバーが検出されました
Web サーバー	**Web** サービスが稼働しています

フォールス・ポジティブの脆弱性について詳しくは、「*IBM Security QRadar Vulnerability Manager* ユーザー・ガイド」を参照してください。

関連概念:

5 ページの『IBM Security QRadar 製品の機能』
IBM Security QRadar 製品資料では、オフェンス、フロー、アセット、ヒストリカル相関などの機能について説明していますが、すべての QRadar 製品でこれらの機能を利用できるわけではありません。使用する製品によっては、説明されている一部の機能をデプロイメントで使用できない場合があります。各製品の機能を確認して、必要な情報を入手してください。

サーバーのディスカバー

「アセット」タブを使用して、ネットワークでサーバーをディスカバーします。

手順

1. 「アセット」タブをクリックします。
2. ナビゲーション・メニューで、「サーバー・ディスカバリー **(Server Discovery)**」をクリックします。

3. 「サーバー・タイプ **(Server Type)**」リストから、ディスカバーするサーバー・タイプを選択します。
4. 以下のいずれかのオプションを選択して、ディスカバーするサーバーを決定します。
   - 現在選択されている「サーバー・タイプ」を使用して、デプロイメント環境のすべてのサーバーを検索するには、「すべて」を選択します。
   - 現在選択されている「サーバー・タイプ」に割り当てられているデプロイメント環境のサーバーを検索するには、「割り当て済み」を選択します。
   - デプロイメント環境の割り当てられていないサーバーを検索するには、「未割り当て」を選択します。
5. 「ネットワーク **(Network)**」リストから、検索するネットワークを選択します。
6. 「サーバーのディスカバー」をクリックします。
7. 「一致するサーバー **(Matching Servers)**」表で、サーバー役割に割り当てるすべてのサーバーのチェック・ボックスを選択します。
8. 「選択したサーバーの承認」をクリックします。

第 16 章 ドメインのセグメンテーション

ネットワークを複数のドメインにセグメント化すると、関連する情報を必要なユーザーのみが使用できるようになります。

セキュリティー・プロファイルを作成すると、当該ドメイン内のユーザー・グループが使用できる情報を制限できます。セキュリティー・プロファイルを使用すると、許可されたユーザーが日常的なタスクの実行に必要な情報のみにアクセスできるようになります。変更を加える際には、各ユーザーを個別に変更するのではなく、影響を受けるユーザーのセキュリティー・プロファイルのみを変更してください。

また、ドメインを使用して IP アドレス範囲のオーバーラップを管理することもできます。この方法は、共有の IBM Security QRadar インフラストラクチャーを使用して複数のネットワークからデータを収集する場合に便利です。ネットワーク上の特定のアドレス・スペースを表すドメインを作成すると、異なるドメインに属する複数のデバイスに同じ IP アドレスを割り当て、それぞれを別個のデバイスとして扱うことができます。

関連概念:

5 ページの『IBM Security QRadar 製品の機能』
IBM Security QRadar 製品資料では、オフェンス、フロー、アセット、ヒストリカル相関などの機能について説明していますが、すべての QRadar 製品でこれらの機能を利用できるわけではありません。使用する製品によっては、説明されている一部の機能をデプロイメントで使用できない場合があります。各製品の機能を確認して、必要な情報を入手してください。

IP アドレスのオーバーラップ

IP アドレスのオーバーラップとは、1 つの IP アドレスが、ネットワーク上にある複数のデバイスまたは論理ユニット (イベント・ソース・タイプなど) に割り当てられていることを意味します。IP アドレスの範囲がオーバーラップしていると、企業買収後に会社がネットワークをマージする場合や、セキュリティー管理サービス・プロバイダー (MSSP) が新規クライアントを導入する場合に重大な問題が発生する可能性があります。

IBM Security QRadar は、さまざまなデバイスから到着するイベントおよびフローの IP アドレスが同じ場合に、それらのイベントおよびフローを区別できなければなりません。複数のイベント・ソースに同じ IP アドレスが割り当てられている場合は、それらを区別するためのドメインを作成します。

例えば、会社 A が会社 B を買収し、QRadar の共有インスタンスを使用して新しい会社のアセットをモニターしたい場合を見てみましょう。買収した会社に同様のネットワーク構造があると、各会社内の異なるログ・ソースに同じ IP アドレスが使用されていることになります。複数のログ・ソースが同じ IP アドレスを持つと、相関、レポート作成、検索、アセット・プロファイルに関する問題の原因となります。

ログ・ソースから QRadar に到着したイベントおよびフローの発生元を区別するには、2 つのドメインを作成し、それぞれのログ・ソースを別々のドメインに割り当てます。必要に応じて、イベントを送信するログ・ソースと同じドメインに各イベント・コレクターとフロー・コレクターを割り当てることもできます。

着信イベントをドメイン別に表示するには、検索を作成し、ドメイン情報を検索結果に含めます。

ドメイン定義およびタグ付け

ドメインは IBM Security QRadar の入力ソースに基づいて定義されます。イベントおよびフローが QRadar に到着すると、ドメイン定義が評価され、イベントおよびフローがドメイン情報でタグ付けされます。

イベントのドメインの指定

イベントのドメインを指定する方法は以下のとおりです。

イベント・コレクター
: イベント・コレクターが特定のネットワーク・セグメントまたは IP アドレス範囲専用の場合は、そのイベント・コレクター全体を当該ドメインの一部としてフラグ設定することができます。

  そのイベント・コレクターに到着するログ・ソースはすべて、このドメインに属します。したがって、新たに自動検出されたログ・ソースは自動的にこのドメインに追加されます。

ログ・ソース
: 特定のログ・ソースがドメインに属するように構成できます。

  このドメインのタグ付け方法はデプロイメント用のオプションです。このオプションでは、イベント・コレクターが複数のドメインからイベントを受信できます。

ログ・ソース・グループ
: ログ・ソース・グループを特定のドメインに割り当てることができます。このオプションでは、ログ・ソース構成に対して幅広い制御が可能になります。

  ログ・ソース・グループに追加された任意の新規ログ・ソースには、そのログ・ソース・グループに関連付けられたドメインのタグが自動的に付与されます。

カスタム・プロパティー
: ログ・ソースからのログ・メッセージにはカスタム・プロパティーを適用できます。

  特定のログ・メッセージが属するドメインを判断するには、ドメイン管理エディター内で定義されたマッピングを対象にカスタム・プロパティーの値が検索されます。

  このオプションは、マルチアドレス範囲またはマルチテナントのログ・ソース (ファイル・サーバー、文書リポジトリーなど) に対して使用されます。

フローのドメインの指定

フローのドメインを指定する方法は以下のとおりです。

フロー・コレクター
: 特定の QFlow コレクターをドメインに割り当てることができます。

  そのフロー・コレクターに到着するフロー・ソースはすべて、このドメインに属します。したがって、新たに自動検出されたフロー・ソースは自動的にこのドメインに追加されます。

フロー・ソース
: 特定のフロー・ソースをドメインに指定することができます。

  このオプションは、1 つの QFlow コレクターが複数のネットワーク・セグメントまたはルーターからフローを収集し、それらのセグメントまたはルーターの IP アドレス範囲がオーバーラップしている場合に便利です。

スキャン結果のドメインの指定

脆弱性スキャナーを特定のドメインに割り当てることもできます。こうすると、スキャン結果がそのドメインに属するものとして適切にフラグ設定されます。ドメイン定義には、すべての QRadar の入力ソースを含めることができます。

事前構成されたドメインにネットワークを割り当てる方法については、 85 ページの『ネットワーク階層』を参照してください。

ドメイン基準を評価する際の優先順位

イベントおよびフローが QRadar システムに到着すると、ドメイン定義の細分度に基づいてドメイン基準が評価されます。

ドメイン定義がイベントに基づく場合は、まず、そのドメイン定義にマップされたすべてのカスタム・プロパティーを対象に着信イベントがチェックされます。カスタム・プロパティーで定義された正規表現の結果がドメイン・マッピングと一致しない場合、このイベントは自動的にデフォルト・ドメインに割り当てられます。

このイベントがカスタム・プロパティーのドメイン定義と一致しない場合は、以下の優先順位が適用されます。

1. ログ・ソース
2. ログ・ソース・グループ
3. イベント・コレクター

ドメインがフローに基づいて定義されている場合は、以下の優先順位が適用されます。

1. フロー・ソース
2. フロー・コレクター

スキャナーに関連付けられたドメインがある場合は、スキャナーによってディスカバーされたすべてのアセットがスキャナーと同じドメインに自動的に割り当てられます。

別の QRadar システムへのデータ転送

データが別の QRadar システムに転送されると、ドメイン情報が削除されます。ドメイン情報が含まれているイベントおよびフローは、受信側の QRadar システム上のデフォルト・ドメインに自動的に割り当てられます。デフォルト・ドメインに割り当てられるイベントおよびフローを特定するために、受信側システムに対するカスタム検索を作成することができます。必要に応じて、これらのイベントおよびフローをユーザー定義ドメインに再度割り当てることもできます。

ドメインの作成

「ドメイン管理」ウィンドウを使用して、IBM Security QRadar の入力ソースに基づくドメインを作成します。

このタスクについて

ドメインの作成時には次のガイドラインを使用してください。

- ユーザー定義ドメインに割り当てられていないものはすべて、自動的にデフォルト・ドメインに割り当てられます。管理特権はすべてのドメインに対する無制限のアクセス権限を付与するため、ドメイン・アクセスが制限されているユーザーには管理特権を付与しないでください。
- 同じカスタム・プロパティーを 2 つの異なるドメインにマップすることは可能ですが、キャプチャー結果はドメインごとに異なっている必要があります。
- 1 つのログ・ソース、ログ・ソース・グループ、またはイベント・コレクターを 2 つの異なるドメインに割り当てることはできません。ログ・ソース・グループがドメインに割り当てられている場合は、マップされた各属性が「ドメイン管理」ウィンドウに表示されます。

セキュリティー・プロファイルを、関連付けたドメインで更新する必要があります。ドメイン・レベルの制限は、セキュリティー・プロファイルが更新され、変更がデプロイされるまで適用されません。

手順

1. 「管理」タブをクリックします。
2. ナビゲーション・メニューで、「システム構成」をクリックします。
3. 「ドメイン管理」をクリックします。
4. ドメインを追加するには、「追加」をクリックして、ドメインの固有の名前と説明を入力します。

   ヒント: 「ドメイン名の入力」検索ボックスに名前を入力すると、固有の名前を確認できます。
5. 定義するドメイン基準に応じて、適切なタブをクリックします。
   - カスタム・プロパティー、ログ・ソース・グループ、ログ・ソース、またはイベント・コレクターに基づいてドメインを定義するには、「イベント」タブをクリックします。
   - フロー・ソースまたはフロー・コレクターに基づいてドメインを定義するには、「フロー」タブをクリックします。

- スキャナー (IBM Security QRadar Vulnerability Managerスキャナーなど) に基づいてドメインを定義するには、「スキャナー」タブをクリックします。

6. カスタム・プロパティーをドメインに割り当てるには、正規表現 (regex) フィルターの結果に一致するテキストを「キャプチャー結果」ボックスに入力します。

   重要: カスタム・イベント・プロパティーを解析して保管するには、「カスタム・イベント・プロパティー」ウィンドウで「ルール、レポート、および検索の構文解析を最適化」チェック・ボックスを選択する必要があります。このオプションにチェック・マークが付いていない場合、ドメインのセグメンテーションは行われません。

7. リストからドメイン基準を選択し、「追加」をクリックします。
8. ソース項目をドメインに追加して、「作成」をクリックします。

次のタスク

セキュリティー・プロファイルを作成して、各ドメインにアクセスできるユーザーを定義します。現在の環境内で最初のドメインを作成したら、すべての非管理ユーザーのセキュリティー・プロファイルを更新して、ドメイン割り当てを指定する必要があります。ドメイン認識環境の場合、セキュリティー・プロファイルにドメイン割り当てが指定されていない非管理ユーザーに対しては、ログ・アクティビティーもネットワーク・アクティビティーも表示されません。

ネットワークの階層構成を確認して、既存の IP アドレスを適切なドメインに割り当てます。詳しくは、 85 ページの『ネットワーク階層』を参照してください。

セキュリティー・プロファイルから導き出されるドメイン特権

セキュリティー・プロファイルを使用してドメイン特権を付与し、IBM Security QRadar システム全体を通してドメイン制限を適用することができます。セキュリティー・プロファイルを使用すると、ビジネス要件が突然変更になった場合でも、大きなユーザー・グループの特権を容易に管理できます。

ユーザーは、各自に割り当てられたセキュリティー・プロファイルに対して設定されたドメイン境界内のデータのみ表示することができます。セキュリティー・プロファイルには、システムへのアクセスを制限するために評価される最初の基準の 1 つとして、ドメインが含まれています。セキュリティー・プロファイルにドメインが割り当てられている場合、そのドメインは他のセキュリティー権限よりも優先されます。ドメイン制限が評価された後、個々のセキュリティー・プロファイルが評価され、特定のプロファイルのネットワーク権限とログ権限が判別されます。

例えば、あるユーザーに、Domain_2 に対する特権とネットワーク 10.0.0.0/8 へのアクセス権限が付与されているとします。このユーザーが表示できるのは、発信元が Domain_2 で、かつ 10.0.0.0/8 ネットワークからのアドレスが含まれているイベント、オフェンス、アセット、およびフローのみです。

QRadar 管理者はすべてのドメインを表示でき、非管理ユーザーにドメインを割り当てることができます。特定のドメインのみに制限するユーザーには、管理特権を割り当てないでください。

セキュリティー・プロファイルを、関連付けたドメインで更新する必要があります。ドメイン・レベルの制限は、セキュリティー・プロファイルが更新されて変更がデプロイされるまで適用されません。

セキュリティー・プロファイルにドメインを割り当てる際には、以下のタイプのドメインへのアクセス権限を付与できます。

ユーザー定義ドメイン
: ドメイン管理ツールを使用して、入力ソースを基準とするドメインを作成できます。詳しくは、『ドメインの作成』を参照してください。

デフォルト・ドメイン
: ユーザー定義ドメインに割り当てられていないものはすべて、自動的にデフォルト・ドメインに割り当てられます。デフォルト・ドメインには、システム規模のイベントが含まれます。

  注: デフォルト・ドメインへのアクセス権限を持つユーザーは、システム規模のイベントを制限なしで表示できます。デフォルト・ドメインのアクセス権限をユーザーに割り当てる前に、このアクセス権限を受け入れ可能な状態にしてください。すべての管理者は、デフォルト・ドメインへのアクセス権限を持ちます。

  共有イベント・コレクター (あるドメインに明示的に割り当てられていないもの) 上で自動ディスカバーされるログ・ソースは、デフォルト・ドメイン上でも自動ディスカバーされます。これらのログ・ソースには、手操作による介入が必要です。これらのログ・ソースを識別するには、ログ・ソース別にグループ化された検索をデフォルト・ドメイン内で定期的に実行する必要があります。

すべてのドメイン
: 「すべてのドメイン」へのアクセス権限を持つセキュリティー・プロファイルに割り当てられたユーザーは、システム内のすべてのアクティブ・ドメイン、デフォルト・ドメイン、およびシステム全体で以前に削除された任意のドメインを表示できます。また、将来作成されるドメインもすべて表示できます。

削除したドメインをセキュリティー・プロファイルに割り当てることはできません。ユーザーに「すべてのドメイン」割り当てが設定されている場合や、そのドメインが削除前にユーザーに割り当てられていた場合、イベント、フロー、アセット、およびオフェンスのヒストリカル検索結果には削除済みドメインが返されます。検索の実行時に、削除済みドメインを基準にフィルタリングすることはできません。

管理ユーザーは、「ドメイン管理」ウィンドウの「サマリー」タブで、セキュリティー・プロファイルに割り当てられたドメインを確認できます。

ドメイン認識環境内でのルール変更

ユーザーが属しているドメインに関係なく、「カスタム・ルールの保守」と「カスタム・ルールの表示」の両方の権限を持つユーザーは、ルールの表示、変更、無効化を行うことができます。

重要**:** ユーザー・ロールに「ログ・アクティビティー」機能を追加すると、「カスタム・ルールの保守」権限および「カスタム・ルールの表示」権限が自動的に付与されます。これらの権限を持つユーザーはすべてのドメインのすべてのログ・データにアクセスでき、セキュリティー・プロファイル設定にドメイン・レベルの制限がある場合でもすべてのドメインのルールを編集できます。ドメイン・ユーザーがログ・データへのアクセスや他のドメインでのルール変更を行えないようにするには、ユーザー・ロールを編集して、「カスタム・ルールの保守」権限と「カスタム・ルールの表示」権限を削除します。

ドメイン認識検索

カスタム検索では、ドメインを検索基準として使用できます。どのドメインを検索対象にするかは、セキュリティー・プロファイルで制御します。

システム規模のイベントと、ユーザー定義ドメインに割り当てられていないイベントは、自動的にデフォルト・ドメインに割り当てられます。管理者、またはデフォルト・ドメインにアクセスできるセキュリティー・プロファイルを持つユーザーは、カスタム検索を作成して、ユーザー定義ドメインに割り当てられていないイベントをすべて表示することができます。

デフォルト・ドメインの管理者は、保存済み検索を他のドメイン・ユーザーと共有できます。ドメイン・ユーザーがこの保存済み検索を実行すると、結果はそのユーザーのドメインに限定されます。

ドメイン固有のルールおよびオフェンス

ルールは、単一ドメインのコンテキストで機能することも、全ドメインのコンテキストで機能することもできます。ドメイン認識ルールには、「次のドメインと一致 **(And Domain Is)**」テストを含めるオプションがあります。

指定されたドメイン内部で発生するイベントにのみ適用されるようにルールを制限することができます。ルールに設定されたドメインとは異なるドメイン・タグを持つイベントは、イベント応答をトリガーしません。

ユーザー定義ドメインを持たない IBM Security QRadar システムでは、ルールによってオフェンスが作成され、そのルールが開始されるたびにそのオフェンスへの寄与が継続されます。ドメイン認識環境では、異なるドメインのコンテキストでルールがトリガーされるたびに、新規のオフェンスが作成されます。

全ドメインのコンテキストで機能するルールは、システム規模のルールと呼ばれます。システム全体で条件をテストするシステム規模のルールを作成するには、「次のドメインと一致 **(And Domain Is)**」テストのドメイン・リストで「任意のドメイン」を選択します。「任意のドメイン」ルールによって「任意のドメイン」オフェンスが作成されます。

単一ドメインのルール
: ルールがステートフル・ルールである場合は、ドメインごとに状態が個別に維持されます。ルールは各ドメインで個別にトリガーされます。ルールがトリガーされると、関連するドメインごとに個別にオフェンスが作成され、各オフェンスにそれらのドメインのタグが付けられます。

単一ドメインのオフェンス
: このオフェンスには、対応するドメイン名を使用したタグが付けられます。これに含めることができるのは、そのドメインでタグ付けされたイベントのみです。

システム規模のルール
: ルールがステートフル・ルールである場合は、システム全体に対して単一の状態が維持され、ドメイン・タグは無視されます。このルールが実行されると、単一のシステム規模のオフェンスを作成するか、またはそのオフェンスに寄与します。

システム規模のオフェンス
: このオフェンスには、「任意のドメイン」のタグが付けられます。これに含めることができるのは、全ドメインでタグ付けされたイベントのみです。

以下の表に、ドメイン認識ルールの例を示します。これらの例では、Domain_A、Domain_B、Domain_C の 3 つのドメインが定義されたシステムを使用します。

QRadar 環境によっては、以下の表に示すルールの例を適用できない場合があります。例えば IBM QRadar Log Manager では、フローとオフェンスを使用するルールを適用できません。

表 52. ドメイン認識ルール

ドメイン・テキスト	説明	ルール応答
ドメインが次のいずれか: **Domain_A**	Domain_A でタグ付けされたイベントのみを認識し、他のドメインでタグ付けされたルールは無視します。	Domain_A でタグ付けされたオフェンスを作成するか、またはこのオフェンスに寄与します。
ドメインが次のいずれか: **Domain_A**、および **HTTP** フローが **1** 分以内に **10** 回検出されたときとして定義されたステートフル・テスト	Domain_A でタグ付けされたイベントのみを認識し、他のドメインでタグ付けされたルールは無視します。	Domain_A でタグ付けされたオフェンスを作成するか、またはこのオフェンスに寄与します。単一状態 (HTTP フロー・カウンター) が Domain_A に対して維持されます。
ドメインが次のいずれか: **Domain_A**、**Domain_B**	Domain_A および Domain_B でタグ付けされたイベントのみを認識し、Domain_C でタグ付けされたルールは無視します。 このルールは、単一ドメイン・ルールの 2 つの独立したインスタンスとして動作し、異なるドメインに対して個別のオフェンスを作成します。	Domain_A でタグ付けされたデータの場合は、Domain_A でタグ付けされた単一ドメインのオフェンスを作成するか、またはこのオフェンスに寄与します。 Domain_B でタグ付けされたデータの場合は、Domain_B でタグ付けされた単一ドメインのオフェンスを作成するか、またはこのオフェンスに寄与します。

表 52. ドメイン認識ルール (続き)

ドメイン・テキスト	説明	ルール応答
ドメインが次のいずれか: **Domain_A**、**Domain_B**、および **HTTP** フローが **1** 分以内に **10** 回検出されたときとして定義されたステートフル・テスト	Domain_A および Domain_B でタグ付けされたイベントのみを認識し、Domain_C でタグ付けされたルールは無視します。 このルールは、単一ドメイン・ルールの 2 つの独立したインスタンスとして動作し、2 つの異なるドメインに対して 2 つの個別の状態 (HTTP フロー・カウンター) を維持します。	このルールが Domain_A でタグ付けされた HTTP フローを 1 分以内に 10 件検出した場合は、Domain_A でタグ付けされたオフェンスを作成するか、またはこのオフェンスに寄与します。 このルールが Domain_B でタグ付けされた HTTP フローを 1 分以内に 10 件検出した場合は、Domain_B でタグ付けされたオフェンスを作成するか、またはこのオフェンスに寄与します。
ドメイン・テストが定義されていない	全ドメインでタグ付けされたイベントを認識し、ドメインごとにオフェンスを作成するか、またはこのオフェンスに寄与します。	各独立ドメインには専用のオフェンスが生成されますが、オフェンスには他のドメインからの寄与は含まれません。
HTTP フローが **1** 分以内に **10** 回検出されたときとして定義されたステートフル・テストがルールにあり、ドメイン・テストが定義されていない	Domain_A、Domain_B、または Domain_C でタグ付けされたイベントを認識します。	ドメインごとに別個の状態を維持し、別個のオフェンスを作成します。
ドメインが次のいずれか: 任意のドメイン	どのドメインでタグ付けされているかにかかわらず、すべてのイベントを認識します。	「**任意のドメイン**」 でタグ付けされた単一のシステム規模のオフェンスを作成するか、またはこのオフェンスに寄与します。
ドメインが次のいずれか: 任意のドメイン、および **HTTP** フローが **1** 分以内に **10** 回検出されたときとして定義されたステートフル・テスト	どのドメインでタグ付けされているかにかかわらず、すべてのイベントを認識し、すべてのドメインに対して単一の状態を維持します。	「**任意のドメイン**」 でタグ付けされた単一のシステム規模のオフェンスを作成するか、またはこのオフェンスに寄与します。 例えば、Domain_A でタグ付けされたイベント 3 件、Domain_B でタグ付けされたイベント 3 件、Domain_C でタグ付けされたイベント 4 件を 1 分以内に検出した場合は、合計で 10 件のイベントが検出されたので、オフェンスが作成されます。

表 52. ドメイン認識ルール (続き)

ドメイン・テキスト	説明	ルール応答
ドメインが次のいずれか: 任意のドメイン、**Domain_A**	「ドメインが次のいずれか: 任意のドメイン」が設定されたルールと同じように機能します。	ドメイン・テストに**「任意のドメイン」**が含まれる場合は、リストされた単一ドメインがすべて無視されます。

オフェンス表を表示する際には、「ドメイン」列をクリックしてオフェンスをソートすることができます。「デフォルト・ドメイン」はソート機能には含まれないため、アルファベット順には表示されません。ただし、列が昇順と降順のどちらでソートされているかに応じて、「ドメイン」リストの先頭または末尾に表示されます。「任意のドメイン」は、オフェンスのリストには表示されません。

例: カスタム・プロパティーに基づくドメイン特権の割り当て

ログ・ファイルに含まれている情報をドメイン定義に使用する場合は、その情報をカスタム・イベント・プロパティーとして公開します。

キャプチャー結果に基づいて、カスタム・プロパティーをドメインに割り当てます。同じカスタム・プロパティーを複数のドメインに割り当てることは可能ですが、キャプチャー結果は異なっている必要があります。

例えば、userID などのカスタム・イベント・プロパティーの評価対象は、単一ユーザーの場合もあればユーザー・リストの場合もあります。各ユーザーは 1 つのドメインにのみ属することができます。

以下の図では、ログ・ソースに含まれるユーザー ID 情報が、カスタム・プロパティー userID として公開されています。イベント・コレクターでは 2 つのユーザー・ファイルが返され、各ユーザーは 1 つのドメインのみに割り当てられています。この場合、1 人のユーザーはドメイン: 9 に割り当てられ、もう 1 人のユーザーはドメイン: 12 に割り当てられています。

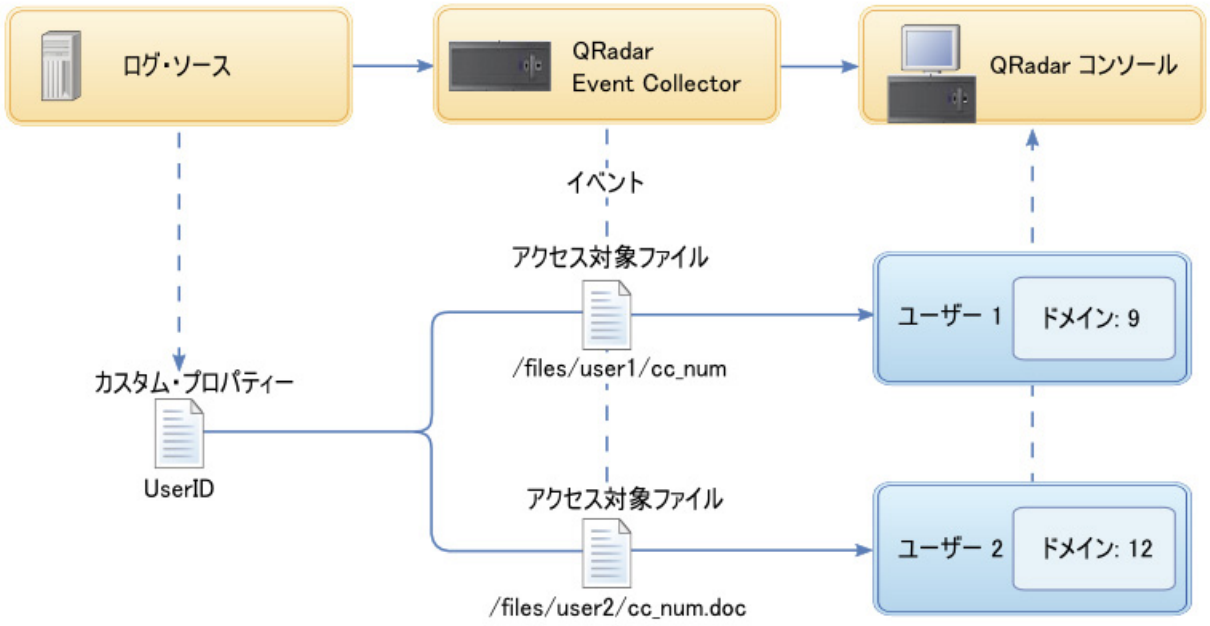


図 *10.* カスタム・イベント・プロパティーを使用したドメインの割り当て

キャプチャー結果に返されたユーザーが特定のユーザー定義ドメインに割り当てられていない場合、そのユーザーは自動的にデフォルト・ドメインに割り当てられます。デフォルト・ドメインの割り当てには、手操作による介入が必要です。デフォルト・ドメイン内のすべてのエンティティーが正しく割り当てられるように、定期的に検索を実行してください。

重要: ドメイン定義内にカスタム・プロパティーを使用する前に、「カスタム・イベント・プロパティー」ウィンドウで「ルール、レポート、および検索の構文解析を最適化」にチェック・マークが付いていることを確認してください。このオプションを使用すると、IBM Security QRadar が当該イベントを始めて受信したときに、カスタム・イベント・プロパティーが解析されてから保管されます。このオプションにチェック・マークが付いていない場合、ドメインのセグメンテーションは行われません。

第 17 章 マルチテナント管理

マルチテナント環境では、マネージド・セキュリティー・サービス・プロバイダー (MSSP) および部門が複数ある組織が、単一の共有の IBM Security QRadar デプロイメントから複数のクライアント組織にセキュリティー・サービスを提供できます。各カスタマーに固有の QRadar インスタンスをデプロイする必要はありません。

マルチテナント・デプロイメントでは、QRadar 入力ソースに基づくドメインを作成することによって、各カスタマーに自身のデータしか表示されないようにしてください。その上で、セキュリティー・プロファイルおよびユーザー・ロールを使用して、ドメイン内の大規模なユーザー・グループに対する特権を管理します。セキュリティー・プロファイルおよびユーザー・ロールにより、ユーザーは、表示が許可されている情報にしかアクセスできなくなります。

関連概念:

5 ページの『IBM Security QRadar 製品の機能』
IBM Security QRadar 製品資料では、オフェンス、フロー、アセット、ヒストリカル相関などの機能について説明していますが、すべての QRadar 製品でこれらの機能を利用できるわけではありません。使用する製品によっては、説明されている一部の機能をデプロイメントで使用できない場合があります。各製品の機能を確認して、必要な情報を入手してください。

マルチテナント環境でのユーザー・ロール

マルチテナント環境には、サービス・プロバイダーと複数のテナントが存在します。ロールはそれぞれ異なる責任を担い、アクティビティーが関連付けられています。

サービス・プロバイダー

サービス・プロバイダーはシステムを所有し、複数のテナントによる利用を管理します。サービス・プロバイダーは、すべてのテナントにわたってデータを確認できます。マネージド・セキュリティー・サービス・プロバイダー (MSSP) 管理者は、通常、以下のアクティビティーを担当します。

- IBM Security QRadar デプロイメントのシステムの正常性を管理およびモニターする。
- 新しいテナントをプロビジョンする。
- テナント管理者およびユーザーのロールおよびセキュリティー・プロファイルを作成する。
- 無許可アクセスからシステムを保護する。
- ドメインを作成してテナント・データを分離する。
- テナント管理者がテナント環境で行った変更をデプロイする。
- QRadar ライセンスをモニターする。
- テナント管理者と共同作業する。

テナント

各テナンシーには、テナント管理者およびテナント・ユーザーが含まれます。テナント組織の職員をテナント管理者にするか、サービス・プロバイダーがカスタマーに代わってテナントを管理することができます。

テナント管理者は以下のアクティビティーを担当します。

- 自身のテナンシー内のネットワーク階層定義を構成する。
- テナント・データを構成および管理する。
- ログ・ソースを表示する。ログ・ソースを編集してデータを統合したり、ログ・ソースを無効化したりすることができる。
- MSSP 管理者と共同作業する。

テナント管理者はテナント固有のデプロイメントを構成できますが、別のテナントの構成にアクセスしたり変更したりすることはできません。QRadar 環境での変更 (自身のテナント内のネットワーク階層の変更を含みます) をデプロイするには、MSSP 管理者に連絡する必要があります。

テナント・ユーザーは管理特権を持たず、アクセスが許可されたデータしか表示できません。例えば、複数のログ・ソースを持つドメイン内の 1 つのログ・ソースのデータのみを表示する特権をユーザーに付与することができます。

マルチテナント環境のドメインおよびログ・ソース

重なり合う IP アドレスを分離したり、イベントやフローなどのデータのソースをテナント固有のデータ・セットに割り当てたりするには、ドメインを使用します。

イベントまたはフローが IBM Security QRadar に到着すると、構成されているドメイン定義を QRadar が評価し、イベントおよびフローがドメインに割り当てられます。テナントは複数のドメインを持つことができます。ドメインが構成されていない場合、イベントおよびフローはデフォルト・ドメインに割り当てられます。

ドメインのセグメンテーション

ドメインは、データのソースに基づいてデータを分離するために使用する仮想的なバケットです。これはマルチテナント環境のためのビルディング・ブロックです。ドメインは以下の入力ソースから構成します。

- イベントおよびフローのコレクター
- フロー・ソース
- ログ・ソースおよびログ・ソース・グループ
- カスタム・プロパティー
- スキャナー

マルチテナント・デプロイメントは、QRadar コンソール 1 つ、集中イベント・プロセッサー 1 つ、およびカスタマーごとに 1 つのイベント・コレクターを含む基本的ハードウェア構成から構成できます。この構成では、コレクター・レベルでドメインを定義します。これにより、QRadar によって受信されたデータが自動的にドメインに割り当てられます。

さらにハードウェア構成を統合する場合は、1 つのコレクターを複数のカスタマーに使用できます。ログまたはフローのソースが同じコレクターによって集約されるが別々のテナントに属する場合は、ソースを別々のドメインに割り当てることができます。ログ・ソース・レベルでドメイン定義を使用する場合は、QRadar デプロイメント全体で各ログ・ソース名が固有でなければなりません。

単一のログ・ソースからのデータを分離して別のドメインに割り当てる必要がある場合は、カスタム・プロパティーからドメインを構成できます。QRadar は、ペイロード内のカスタム・プロパティーを検索して正しいドメインに割り当てます。例えば、Check Point Provider-1 デバイスと統合するように QRadar を構成した場合は、カスタム・プロパティーを使用して、そのログ・ソースからのデータを別のドメインに割り当てることができます。

自動ログ・ソース検出

ドメインがコレクター・レベルで定義され、かつ専用のイベント・コレクターが単一のドメインに割り当てられている場合は、自動的に検出された新規ログ・ソースがそのドメインに割り当てられます。例えば、`Event_Collector_1` で検出されたすべてのログ・ソースが `Domain_A` に割り当てられます。`Event_Collector_2` で自動的に収集されたログ・ソースは、すべて `Domain_B` に割り当てられます。

ドメインがログ・ソースまたはカスタム・プロパティーのレベルで定義されている場合、自動的に検出されたがまだドメインに割り当てられていないログ・ソースは自動的にデフォルト・ドメインに割り当てられます。MSSP 管理者がデフォルト・ドメインのログ・ソースを確認し、正しいクライアント・ドメインに割り振る必要があります。マルチテナント環境でログ・ソースを特定のドメインに割り当てると、データ漏えいを防止でき、ドメイン間でのデータ分離を実現できます。

新規テナントのプロビジョン

マネージド・セキュリティー・サービス・プロバイダー (MSSP) 管理者は、IBM Security QRadar の単一のインスタンスを使用して、脅威の検出と優先順位付けのための統一アーキテクチャーを複数のカスタマーに提供します。

このシナリオでは、新しいクライアントをオンボードします。新しいテナントをプロビジョンし、専用のテナント内で限定された管理義務を果たすテナント管理者アカウントを作成します。テナント管理者のアクセスを制限して、他のテナントの情報を参照および編集できないようにします。

新しいテナントをプロビジョンする前に、カスタマーのデータ・ソース (ログ・ソースやフロー・コレクターなど) を作成してドメインに割り当てる必要があります。

QRadar に新しいテナントをプロビジョンするには、「管理」タブのツールを使用して以下の作業を行います。

1. テナントを作成するために、「テナント管理」をクリックします。

   各テナントに対する 1 秒当たりのイベント数 (EPS) と 1 分当たりのフロー数 (FPM) の制限の設定について詳しくは、 268 ページの『マルチテナント・デプロイメントでのライセンス使用状況のモニター』を参照してください。

2. ドメインをテナントに割り当てるために、「ドメイン管理」をクリックします。
3. テナント管理者のロールを作成して「代行管理」権限を付与するために、「ユーザー・ロール」をクリックします。

   マルチテナント環境では、「代行管理」権限を持つテナント・ユーザーは自身のテナント環境のデータしか参照できません。「代行管理」に属さない他の管理権限を割り当てると、アクセスがそのドメインに制限されることがなくなります。
4. テナント・セキュリティー・プロファイルを作成し、テナント・ドメインの指定によってデータ・アクセスを制限するために、「セキュリティー・プロファイル」をクリックします。
5. テナント・ユーザーを作成してユーザー・ロール、セキュリティー・プロファイル、およびテナントを割り当てるために、「ユーザー」をクリックします。

マルチテナント・デプロイメントでのライセンス使用状況のモニター

マネージド・セキュリティー・サービス・プロバイダー (MSSP) 管理者は、IBM Security QRadar デプロイメント全体のイベント・レートおよびフロー・レートをモニターします。

テナントを作成するときには、1 秒当たりのイベント数 (EPS) と 1 分当たりのフロー数 (FPM) の両方の制限を設定できます。テナントごとに EPS および FPM の制限を設定すると、複数のクライアントにわたってライセンス・キャパシティーを詳細に管理できます。プロセッサーが単一のカスタマーのイベントまたはフローを収集する場合は、テナントの EPS および FPM の制限を割り当てる必要はありません。単一のプロセッサーで複数のカスタマーのイベントまたはフローを収集する場合は、テナントごとに EPS および FPM の制限を設定できます。

EPS および FPM の制限を、ソフトウェア・ライセンスまたはアプライアンス・ハードウェアのいずれかの制限を超える値に設定した場合は、その制限を超えないように、そのテナントのイベントおよびフローが自動的に抑制されます。テナントに EPS および FPM の制限を設定しない場合は、ライセンス制限またはアプライアンス制限のいずれかに達するまで、各テナントがイベントおよびフローを受信します。ライセンス制限は管理対象ホストに適用されます。通常の運用でライセンス制限を超えてしまう場合は、デプロイメントに適した別のライセンスを取得できます。

デプロイメント内の累積ライセンス制限の表示

テナントごとに設定する EPS および FPM のレートが、ライセンス資格に照らして自動的に検証されることはありません。システムに適用されるソフトウェア・ライセンスの累積制限をアプライアンスのハードウェア制限と比較するには、以下の手順を実行します。

1. 「管理」タブで、「システム構成」 > 「システムおよびライセンス管理」をクリックします。
2. 「デプロイメントの詳細」を展開し、「イベント制限」または「フロー制限」にマウス・ポインターを合わせます。

ログ・ソースごとの EPS レートの表示

「拡張検索」フィールドを使用して Ariel 照会言語 (AQL) の照会を入力すると、ログ・ソースの EPS レートが表示されます。

1. 「ログ・アクティビティー」タブで、「検索」ツールバー上のリストから「拡張検索」を選択します。
2. ログ・ソースごとの EPS を表示するには、「拡張検索」フィールドに以下の AQL 照会を入力します。

```
select logsourcename(logsourceid) as LogSource, sum(eventcount) /
( ( max(endTime) - min(startTime) ) / 1000 ) as EPS from events
group by logsourceid order by EPS desc last 24 hours
```

(endTime) および (startTime) の日付値は、UNIX のエポック 1970 年 1 月 1 日からの、ミリ秒単位の時間で表す必要があります。

ドメインごとの EPS レートの表示

「拡張検索」フィールドを使用して Ariel 照会言語 (AQL) の照会を入力すると、ドメインの EPS レートが表示されます。

1. 「ログ・アクティビティー」タブで、「検索」ツールバーのドロップダウン・リスト・ボックスから「拡張検索」を選択します。
2. ドメインごとの EPS を表示するには、「拡張検索」フィールドに以下の AQL 照会を入力します。

```
select DOMAINNAME(domainid) as LogSource, sum(eventcount) /
( ( max(endTime) - min(startTime)) / 1000 ) as EPS from events
group by domainid order by EPS desc last 24 hours
```

(endTime) および (startTime) の日付値は、UNIX のエポック 1970 年 1 月 1 日からの、ミリ秒単位の時間で表す必要があります。

ログ・ソースの平均 EPS レートのみを表示する場合は、「管理」タブで「データ・ソース」ペインの「ログ・ソース」をクリックします。これを使用して、レポートが失敗しているログ・ソースの構成の問題を素早く識別することができます。

デプロイメント内の個別ライセンス制限の表示

テナントごとに設定する EPS および FPM のレートが、ライセンス資格に照らして自動的に検証されることはありません。システムに適用されるソフトウェア・ライセンスの個別制限をアプライアンスのハードウェア制限と比較して表示するには、以下の手順を実行します。

1. 「管理」タブで、「システム構成」 > 「システムおよびライセンス管理」をクリックします。
2. 「デプロイメントの詳細」を展開し、「イベント制限」または「フロー制限」にマウス・ポインターを合わせます。

個別ログ・ソースの EPS レートの表示

「拡張検索」フィールドを使用して Ariel 照会言語 (AQL) の照会を入力すると、個別ログ・ソースの EPS レートが表示されます。

1. PSQL 照会を使用してログ・ソース ID を取得します。

a. SSH を使用して、QRadar に管理者としてログインします。
b. 以下のコマンドを使用して PSQL にアクセスします。

```
psql -U qradar
```

c. 以下のコマンドを使用して、ログ・ソース名およびログ・ソース ID のリストを取得します。

```
select id,devicename from sensordevice;
```

d. リストからログ・ソース ID を選択します。

2. 「ログ・アクティビティー」タブで、「検索」ツールバー上のリストから「拡張検索」を選択します。
3. 選択したログ・ソースの EPS レートを表示するには、「拡張検索」フィールドに以下の AQL 照会を入力します。

```
select logsourcename(logsourceid) as LogSource, sum(eventcount) /
( ( max(endTime) -  min(startTime) ) / 1000 ) as EPS from events
where logsourceid=logsourceid
group by logsourceid order by EPS desc last 24 hours
```

(endTime) および (startTime) の日付値は、UNIX のエポック 1970 年 1 月 1 日からの、ミリ秒単位の時間で表す必要があります。

個別ドメインの EPS レートの表示

「拡張検索」フィールドを使用して Ariel 照会言語 (AQL) の照会を入力すると、個別ドメインの EPS レートが表示されます。

1. PSQL 照会を使用してドメイン ID を取得します。
   a. SSH を使用して、QRadar に管理者としてログインします。
   b. 以下のコマンドを使用して PSQL にアクセスします。

```
psql -U qradar
```

   c. 以下のコマンドを使用して、ドメイン名およびドメイン ID のリストを取得します。

```
select id, name from domains;
```

   d. リストからドメイン ID を選択します。
2. 「ログ・アクティビティー」タブで、「検索」ツールバー上のリストから「拡張検索」を選択します。
3. 選択したドメインの EPS レートを表示するには、「拡張検索」フィールドに以下の AQL 照会を入力します。

```
select DOMAINNAME(domainid) as LogSource, sum(eventcount) /
( ( max(endTime) - min(startTime)) / 1000 ) as EPS from events where
domainid=domainid
group by domainid order by EPS desc last 24 hours
```

(endTime) および (startTime) の日付値は、UNIX のエポック 1970 年 1 月 1 日からの、ミリ秒単位の時間で表す必要があります。

ドロップされたイベントおよびフローの検出

IBM Security QRadar の処理パイプラインが多量の着信イベントおよびフローを処理できない場合、またはイベントおよびフローの数がデプロイメントのライセンス

制限を超えた場合、イベントおよびフローがドロップされます。このような状態が発生した場合、QRadar のログ・ファイル・メッセージを確認できます。

手順

1. SSH を使用して、root ユーザーとして QRadar にログインします。
2. /var/log/qradar.error ログ・ファイルを表示し、以下のメッセージを見つけます。

   以下のメッセージは、イベントまたはフローがドロップされたことを示します。

   ```
   [テナント:[テナント ID]:[テナント名]
   テナント・イベント・スロットル・キューへの追加試行中にイベントがドロップされました。
   (Event dropped while attempting to add to Tenant Event Throttle queue.)
   テナント・イベント・スロットル・キューがいっぱいです。
   (The Tenant Event Throttle queue is full.)
   ```

   ```
   [テナント:[テナント ID]:[テナント名]
   テナント・フロー・スロットル・キューへの追加試行中にフローがドロップされました。
   (Flow dropped while attempting to add to Tenant Flow Throttle queue.)
   テナント・フロー・スロットル・キューがいっぱいです。
   (The Tenant Flow Throttle queue is full.)
   ```

   以下のメッセージは、処理パイプラインがキャパシティーの限界に近いことを示します。

   ```
   スロットル・プロセッサーがイベントに対応できません。
   (Throttle processor cannot keep up with events.)
   TENANT_QUEUE_THREAD_INTERVAL_IN_MILLISEC が短すぎます。
   (TENANT_QUEUE_THREAD_INTERVAL_IN_MILLISEC is probably too short.)
   ```

   ```
   スロットル・プロセッサーがフローに対応できません。
   (Throttle processor cannot keep up with flows.)
   TENANT_QUEUE_THREAD_INTERVAL_IN_MILLISEC が短すぎます。
   (TENANT_QUEUE_THREAD_INTERVAL_IN_MILLISEC is probably too short.)
   ```

   この警告が継続する場合、QRadar でイベントまたはフローがドロップされる可能性があります。

次のタスク

システムでイベントおよびフローがドロップされる場合、多くのデータを処理できるようにライセンスを拡張すること、またはテナントごとにより厳格な EPS 制限および FPM 制限を設定することができます。

マルチテナント・デプロイメントでのルール管理

マルチテナント環境では、ルールをカスタマイズしてテナント認識ルールにする必要があります。テナント認識ルールは、「ドメインが次のいずれかである場合 **(when the domain is one of the following)**」ルール・テストを使用しますが、ドメイン修飾子によってルールの有効範囲が決定されます。

マルチテナント・デプロイメントでドメイン修飾子を使用してルールの有効範囲を変更する方法を以下の表に示します。

表 53. マルチテナント環境でのルールの有効範囲

ルールの有効範囲	説明	ルール・テストの例
単一ドメイン・ルール	このルールにはドメイン修飾子が 1 つしか含まれません。	かつドメインが次のいずれかである場合: **(and when the domain is one of the following:)** *manufacturing*
単一テナント・ルール	このルールには、テナントに割り当てられたすべてのドメインが含まれます。単一テナント・ルールは、単一のテナント内の複数のドメイン全体にわたってイベントを相関させるために使用します。	かつドメインが次のいずれかである場合: **(and when the domain is one of the following:)** *manufacturing, finance, legal*
グローバル・ルール	このルールは「任意のドメイン」修飾子を使用し、すべてのテナントにわたって実行されます。	かつドメインが次のいずれかである場合: **(and when the domain is one of the following:)** 任意のドメイン

ドメイン認識にすると、カスタム・ルール・エンジン (CRE) は、テナントの各ドメインを使用することで、異なるテナントからのイベント相関を分離します。ドメインに分割されたネットワークでのルールの処理について詳しくは、 253 ページの『第 16 章 ドメインのセグメンテーション』を参照してください。

テナント・ユーザーのログ・アクティビティー機能の制限

テナントの管理者およびユーザーがそれぞれのテナントについてのみログ・データを表示できるようにするには、「ログ・アクティビティー」機能の権限を制限する必要があります。

このタスクについて

ユーザー・ロールに「ログ・アクティビティー」機能を追加すると、「カスタム・ルールの保守」権限および「カスタム・ルールの表示」権限が自動的に付与されます。これらの権限があるユーザーは、すべてのドメインのすべてのログ・データにアクセスできます。セキュリティー・プロファイルの設定にドメイン・レベルの制限があっても、すべてのドメインのルールを編集できます。

ユーザーが他のドメインまたはテナントのログ・データへのアクセスおよびルールの変更をできないようにするには、ユーザー・ロールを編集して、「カスタム・ルールの保守」権限と「カスタム・ルールの表示」権限を削除します。これらの権限がない場合、テナントの管理者およびユーザーはルール (自分のドメインのルールを含む) を変更できません。

手順

1. 「管理」タブをクリックします。
2. ナビゲーション・メニューで、「システム構成」をクリックします。
3. 「ユーザー・ロール」をクリックし、編集するユーザー・ロールを選択します。
4. 「ログ・アクティビティー」で、「カスタム・ルールの保守」チェック・ボックスおよび「カスタム・ルールの表示」チェック・ボックスをクリアします。

5. 「保存」をクリックします。

マルチテナント・デプロイメントでのネットワーク階層の更新

IBM Security QRadar は、ネットワーク階層を使用して、環境内のネットワーク・トラフィックを把握し、分析します。

「ネットワーク階層の定義」権限を持つテナント管理者は、自身のテナント内のネットワーク階層を変更できます。

ネットワーク階層を変更するには、QRadar 環境ですべての構成をデプロイして更新を適用する必要があります。すべての構成をデプロイすると、すべての QRadar サービスが再始動され、デプロイが完了するまでイベントおよびフローのデータ収集が停止します。テナント管理者は、変更をデプロイするためにマネージド・セキュリティー・サービス・プロバイダー (MSSP) に連絡する必要があります。MSSP 管理者が、計画停止の間にデプロイするように計画し、事前にすべてのテナント管理者に通知することができます。

マルチテナント環境では、デプロイメント全体でネットワーク・オブジェクト名が固有でなければなりません。ネットワーク・オブジェクトを別のドメインに割り当てる場合であっても、同じ名前のネットワーク・オブジェクトを使用することはできません。

関連概念:

85 ページの『ネットワーク階層』

IBM Security QRadar は、ネットワーク階層のオブジェクトおよびグループを使用して、ネットワーク・アクティビティーを表示したり、ネットワーク内のグループやサービスをモニターします。

テナントの保存ポリシー

共有データに対して最大 10 個の保存バケットを構成でき、各テナントに対して最大 10 個の保存バケットを構成できます。保存バケットを構成するまで、すべてのイベントおよびフローは、各テナントのデフォルトの保存バケットに保管されます。

10 件を超えるテナントが QRadar デプロイメントに存在する場合は、共有データ保存ポリシーを構成し、続いてドメイン・フィルターを使用して、テナント内のドメインごとにドメイン・ベースの保存ポリシーを作成することができます。ドメインを追加すると、そのテナントのデータのみにポリシーを適用するように指定されます。

保存ポリシーの作成について詳しくは、 120 ページの『データ保存』を参照してください。

第 18 章 アセットの管理

ネットワーク内のサーバーおよびホストに対して作成されるアセットおよびアセット・プロファイルにより、セキュリティーの問題を解決する際に役に立つ重要な情報が提供されます。アセット・データを使用すると、システムでトリガーされたオフェンスを物理アセットまたは仮想アセットに関連付けて、セキュリティー調査の開始点を用意できます。

IBM Security QRadar の「アセット」タブには、ネットワーク内のアセットに関する既知の情報の統合ビューが用意されています。QRadar が詳しい情報をディスカバーすると、システムによりアセット・プロファイルが更新され、アセットの完全な実態が徐々に作り上げられていきます。

アセット・プロファイルは、イベント・データまたはフロー・データから受動的に抽出されたアイデンティティー情報から、または QRadar が脆弱点スキャン中に能動的にルックアップしたデータから動的に作成されます。アセット・データをインポートすることや、アセット・プロファイルを手動で編集することもできます。詳しくは、「*IBM Security QRadar* ユーザー・ガイド」のトピック『アセット・プロファイルのインポート』および『アセット・プロファイルの追加または編集』を参照してください。

制約事項**:** IBM Security QRadar Vulnerability Manager がインストールされている場合に限り、IBM QRadar Log Manager はアセット・データを追跡します。QRadar SIEM と QRadar Log Manager の差異について詳しくは、 5 ページの『IBM Security QRadar 製品の機能』を参照してください。

関連概念:

5 ページの『IBM Security QRadar 製品の機能』

IBM Security QRadar 製品資料では、オフェンス、フロー、アセット、ヒストリカル相関などの機能について説明していますが、すべての QRadar 製品でこれらの機能を利用できるわけではありません。使用する製品によっては、説明されている一部の機能をデプロイメントで使用できない場合があります。各製品の機能を確認して、必要な情報を入手してください。

アセット・データの送信元

アセット・データは、IBM Security QRadar デプロイメント内の複数の異なるソースから受信されます。

アセット・データはアセット・データベースに増分的に書き込まれます。通常は 2、3 個のデータが同時に書き込まれます。ネットワーク脆弱性スキャナーからの更新を除き、各アセット更新に含まれる情報は、一度に 1 つのアセットについてのみです。

アセット・データは、通常は以下のいずれかのアセット・データ・ソースから生じます。

イベント

イベント・ペイロード (DHCP または認証サーバーによって作成されたものなど) には、多くの場合、ユーザー・ログイン、IP アドレス、ホスト名、MAC アドレス、その他のアセット情報が含まれています。このデータは即時にアセット・データベースに提供され、アセット更新の適用先となるアセットを判別するのに役立ちます。

イベントは、異常なアセット増加の主要な原因です。

フロー

フロー・ペイロードには、一定の構成可能間隔で収集された IP アドレス、ポート、およびプロトコルなどの通信情報が含まれています。各間隔の終わりに、データは一度に 1 つの IP アドレスずつ、アセット・データベースに提供されます。

フローからのアセット・データは単一の ID である IP アドレスに基づいてアセットとペアにされるため、フロー・データが異常なアセット増加の原因となることはありません。

脆弱性スキャナー

QRadar には、IBM 提供とサード・パーティー提供の両方の脆弱性スキャナーが組み込まれています。それらの脆弱性スキャナーは、オペレーティング・システム、インストール済みソフトウェア、およびパッチ情報などのアセット・データを提供できます。データのタイプはスキャナーごとに異なっており、スキャンごとに異なる場合もあります。新規アセット、ポート情報、および脆弱性が検出されると、スキャンで定義されている CIDR 範囲に基づいて、データがアセット・プロファイルに入ります。

スキャナーが異常なアセット増加の原因となる可能性もありますが、まれです。

ユーザー・インターフェース

アセット・ロールを持つユーザーは、アセット情報をアセット・データベースに直接インポートまたは提供できます。ユーザーが直接提供するアセット更新は、特定のアセットを対象としたものであるため、アセット調整ステージはバイパスされます。

ユーザーによって提供されるアセット更新は、異常なアセット増加の原因にはなりません。

ドメイン認識アセット・データ

アセット・データ・ソースがドメイン情報で構成されると、そのデータ・ソースから生じるすべてのアセット・データは、同じドメインで自動的にタグ付けされます。アセット・モデル内のデータはドメインを認識するため、ドメイン情報は、アイデンティティー、オフェンス、アセット・プロファイル、およびサーバー・ディスカバリーを含む、すべての QRadar コンポーネントに適用されます。

アセット・プロファイルを表示すると、一部のフィールドがブランクである場合があります。ブランクのフィールドが存在するのは、システムがその情報をアセット更新で受け取っていない場合か、または情報がアセット保存期間を超過している場合です。デフォルトの保存期間は 120 日です。 IP アドレスが 0.0.0.0 と表示される場合は、アセットに IP アドレス情報が含まれていないことを示します。

受信アセット・データのワークフロー

IBM Security QRadar は、イベント・ペイロードでアイデンティティー情報を使用して、新規アセットを作成するかまたは既存のアセットを更新するかを決定します。

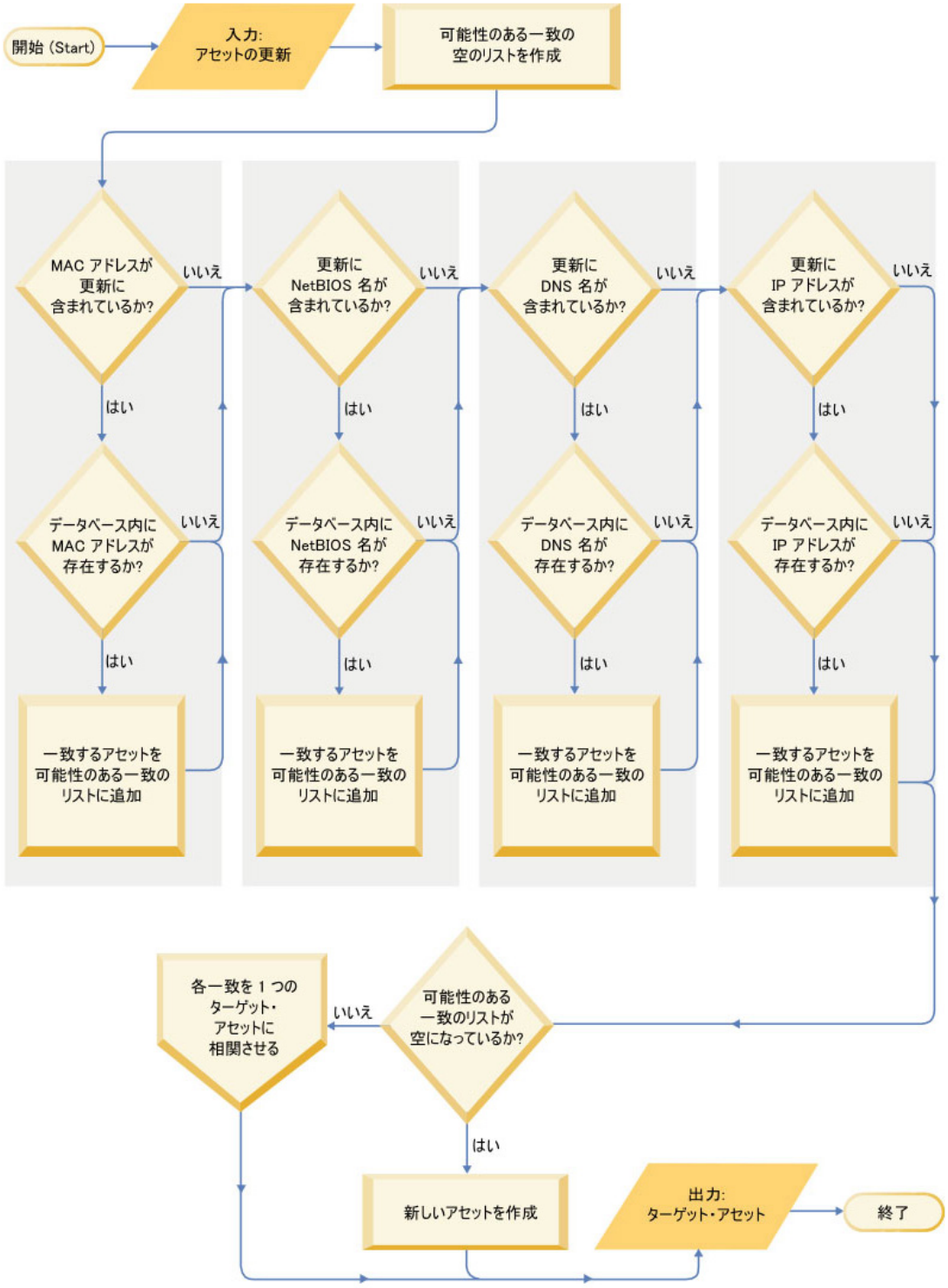


図 *11.* アセット・データ・ワークフローの図

1. QRadar はイベントを受け取ります。アセット・プロファイラーは、アイデンティティー情報についてイベント・ペイロードを調べます。
2. アイデンティティー情報に、アセット・データベース内のアセットと既に関連付けられている MAC アドレス、NetBIOS ホスト名、または DNS ホスト名が含まれている場合、そのアセットは新しい情報があればその情報で更新されます。
3. 入手できるアイデンティティー情報が IP アドレスのみである場合、システムは同じ IP アドレスを持つ既存のアセットに対する更新を調整します。
4. アセット更新に、既存のアセットに一致する IP アドレスが含まれているが、他のアイデンティティー情報は既存のアセットと一致しない場合、システムは他の情報を使用してフォールス・ポジティブ一致を除外してから、既存のアセットを更新します。
5. アイデンティティー情報がデータベース内の既存のアセットと一致しない場合、イベント・ペイロードの情報に基づいて新規アセットが作成されます。

アセット・データへの更新

IBM Security QRadar は、イベント・ペイロードでアイデンティティー情報を使用して、新規アセットを作成するかまたは既存のアセットを更新するかを決定します。

各アセット更新には、単一のアセットに関するトラステッド情報が含まれている必要があります。 QRadar がアセット更新を受信すると、その更新の適用先となるアセットがシステムよって判別されます。

アセット調整 とは、アセット更新とアセット・データベース内の関連アセットとの間の関係を判別するプロセスのことです。アセット調整は、QRadar が更新を受け取った後から、アセット・データベースに情報が書き込まれる前までの期間内に実行されます。

アイデンティティー情報

すべてのアセットには、少なくとも 1 つのアイデンティティー・データが含まれている必要があります。その同じアイデンティティー・データが 1 つ以上含まれている後続の更新は、そのデータを所有するアセットで調整されます。 IP アドレスに基づく更新は、フォールス・ポジティブのアセット一致を回避するために注意深く処理されます。フォールス・ポジティブのアセット一致は、1 つの物理アセットに、システム内の別のアセットが以前に所有していた IP アドレスの所有権が割り当てられているときに起きます。

複数のアイデンティティー・データが含まれている場合、アセット・プロファイラーは以下の順序 (最も確度の高いデータから最も確度の低いデータの順) で情報に優先順位を付けます。

- MAC アドレス
- NetBIOS ホスト名
- DNS ホスト名
- IP アドレス

MAC アドレス、NetBIOS ホスト名、DNS ホスト名はそれぞれ固有の値であるため、確度の高いアイデンティティー・データとみなされます。受け取った更新で、IP アドレスしか既存のアセットと一致しないものは、より限定的なアイデンティティー・データと一致する更新とは異なる方法で処理されます。

アセット調整除外ルール

IBM Security QRadar が受け取る各アセット更新では、アセット調整除外ルールにより、アセット更新の MAC アドレス、NetBIOS ホスト名、DNS ホスト名、および IP アドレスに対してテストが適用されます。

デフォルトでは、各アセット・データが追跡される期間は 2 時間です。アセット更新内のいずれかのアイデンティティー・データが 2 時間以内に複数回の疑わしい振る舞いを示す場合、そのデータはアセット・ブラックリストに追加されます。テストされるアイデンティティー・アセット・データのタイプごとに、新しいブラックリストが作成されます。

ドメイン認識環境では、アセット調整除外ルールは、ドメインごとにアセット・データの振る舞いを別個に追跡します。

アセット調整除外ルールは、以下のシナリオをテストします。

表 *54.* ルールのテストおよび対応

シナリオ	ルール応答
MAC アドレスが 2 時間以内に 3 つ以上の異なる IP アドレスに関連付けられる場合	MAC アドレスをアセット調整ドメイン MAC ブラックリストに追加する
DNS ホスト名が 2 時間以内に 3 つ以上の異なる IP アドレスに関連付けられる場合	DNS ホスト名をアセット調整ドメイン DNS ブラックリストに追加する
NetBIOS ホスト名が 2 時間以内に 3 つ以上の異なる IP アドレスに関連付けられる場合	NetBIOS ホスト名をアセット調整ドメイン NetBIOS ブラックリストに追加する
IPv4 アドレスが 2 時間以内に 3 つ以上の異なる MAC アドレスに関連付けられる場合	IP アドレスをアセット調整ドメイン IPv4 ブラックリストに追加する
NetBIOS ホスト名が 2 時間以内に 3 つ以上の異なる MAC アドレスに関連付けられる場合	NetBIOS ホスト名をアセット調整ドメイン NetBIOS ブラックリストに追加する
DNS ホスト名が 2 時間以内に 3 つ以上の異なる MAC アドレスに関連付けられる場合	DNS ホスト名をアセット調整ドメイン DNS ブラックリストに追加する
IPv4 アドレスが 2 時間以内に 3 つ以上の異なる DNS ホスト名に関連付けられる場合	IP アドレスをアセット調整ドメイン IPv4 ブラックリストに追加する
NetBIOS ホスト名が 2 時間以内に 3 つ以上の異なる DNS ホスト名に関連付けられる場合	NetBIOS ホスト名をアセット調整ドメイン NetBIOS ブラックリストに追加する
MAC アドレスが 2 時間以内に 3 つ以上の異なる DNS ホスト名と関連付けられる場合	MAC アドレスをアセット調整ドメイン MAC ブラックリストに追加する

表 54. ルールのテストおよび対応 (続き)

シナリオ	ルール応答
IPv4 アドレスが 2 時間以内に 3 つ以上の異なる NetBIOS ホスト名に関連付けられる場合	IP アドレスをアセット調整ドメイン IPv4 ブラックリストに追加する
DNS ホスト名が 2 時間以内に 3 つ以上の異なる NetBIOS ホスト名に関連付けられる場合	DNS ホスト名をアセット調整ドメイン DNS ブラックリストに追加する
MAC アドレスが 2 時間以内に 3 つ以上の異なる NetBIOS ホスト名に関連付けられる場合	MAC アドレスをアセット調整ドメイン MAC ブラックリストに追加する

これらのルールは、「オフェンス」タブで、「ルール」をクリックし、ドロップダウン・リストで「アセット調整除外」グループを選択することで表示できます。

アセットのマージ

アセットのマージ とは、別々のアセットの情報を、それらが実際には同じ物理アセットであるという前提の下に結合させるプロセスのことです。

アセットのマージは、アセット更新に、2 つの異なるアセット・プロファイルと一致するアイデンティティー・データが含まれているときに実行されます。例えば、あるアセット・プロファイルと一致する NetBIOS ホスト名と、別のアセット・プロファイルと一致する MAC アドレスが単一の更新に含まれていると、アセットのマージが開始されることがあります。

システムによっては、2 つの異なる物理アセットからのアイデンティティー情報を単一のアセット更新に誤って結合してしまうアセット・データ・ソースがあるため、大量のアセットのマージが行われる可能性があります。このようなシステムの例としては、以下のような環境があります。

- イベント・プロキシーとして機能する中央 Syslog サーバー
- 仮想マシン
- 自動化されたインストール済み環境
- iPad や iPhone などのアセットに共通の、固有でないホスト名
- 共有 MAC アドレスがある仮想プライベート・ネットワーク
- アイデンティティー・フィールドが `OverrideAndAlwaysSend=true` であるログ・ソース拡張

多くの IP アドレス、MAC アドレス、またはホスト名があるアセットは、アセット増大での逸脱を示し、システム通知が起動する場合があります。

異常なアセット増加の識別

IBM Security QRadar では、アセット・データ・ソースによって作成される更新を適切に処理するために、手動での修復が必要となることがあります。異常なアセット増加の原因に応じて、問題の原因となっているアセット・データ・ソースを修正するか、またはそのデータ・ソースからのアセット更新をブロックすることができます。

異常なアセット増加 は、単一のデバイスに対するアセット更新の数が、特定のアイデンティティー情報タイプの保存しきい値によって設定されている制限を超えた場合に発生します。異常なアセット増加に適切に対処することは、正確なアセット・モデルを維持する上で重要です。

異常なアセット増加が発生する原因は、アセット・モデルを更新するには信頼できないデータが含まれているアセット・データ・ソースにあります。異常なアセット増加が発生している可能性が検出されたら、その情報源を調べ、そのアセットで大量のアイデンティティー・データが集計される適切な理由があるかどうかを判断します。異常なアセット増加の原因は環境によって異なります。

DHCP サーバーのアセット・プロファイルでの不自然なアセット増大の例

動的ホスト構成プロトコル (DHCP) ネットワーク内の仮想プライベート・ネットワーク (VPN) サーバーについて考えてみます。 VPN サーバーは、着信 VPN クライアントに対して、そのクライアントの代わりに DHCP 要求をネットワークの DHCP サーバーに委任することで、IP アドレスを割り当てるように構成されています。

DHCP サーバーからすると、同じ MAC アドレスが多くの IP アドレス割り当てを繰り返し要求しているように見えます。ネットワーク操作のコンテキストでは、VPN サーバーは IP アドレスをクライアントに委任しますが、DHCP サーバー側では要求が代理の別のアセットによって出されたとしても区別できません。

DHCP サーバー・ログ (QRadar ログ・ソースとして構成される) は、VPN サーバーの MAC アドレスと、VPN クライアントに割り当てられた IP アドレスを関連付ける、DHCP 確認応答 (DHCP ACK) イベントを生成します。アセット調整が行われるときに、システムはこのイベントを MAC アドレスにより調整します。この結果、単一の既存のアセットで、解析される DHCP ACK イベントごとに IP アドレスが 1 つ増えることになります。

最終的に、1 つのアセット・プロファイルに、VPN サーバーに割り振られたすべての IP アドレスが含まれることになります。この異常なアセット増加は、複数のアセットに関する情報が含まれるアセット更新が原因で起きます。

しきい値の設定

データベース内のアセットのプロパティーが特定の数に達すると (複数の IP アドレスや複数の MAC アドレスなど)、QRadar はアセットがそれ以上の更新を受け取らないようにブロックします。

アセットの更新をブロックする条件は、アセット・プロファイラーのしきい値設定で指定します。アセットはこのしきい値に達するまでは、正常に更新されます。システムがしきい値を超えるのに十分なデータを収集すると、アセットは異常なアセット増加を示すようになります。アセットに対するそれ以降の更新は、増大逸脱が修正されるまでブロックされます。

異常なアセット増加を示すシステム通知

IBM Security QRadar は、環境内の異常なアセット増加を特定および管理できるようにする目的で、システム通知を生成します。

次のシステム・メッセージは、QRadar で異常なアセット増加が発生している可能性が確認されたことを示します。

- `The system detected asset profiles that exceed the normal size threshold`
- `The asset blacklist rules have added new asset data to the asset blacklists`

システム通知メッセージには、異常な増加が発生しているアセットを特定する上で役立つレポートへのリンクが含まれています。

頻繁に変化するアセット・データ

アセットの増加は、大量のアセット・データが正当な理由で変更されることが原因で発生することがあります。次にそのような状況の例を示します。

- オフィス間を頻繁に移動するモバイル・デバイスには、ログインするたびに新しい IP アドレスが割り当てられます。
- 大学構内など、IP アドレス・リースが短い公衆 WiFi に接続するデバイスは、1 学期の間に大量のアセット・データを収集することがあります。

例: ログ・ソース拡張の構成エラーが異常なアセット増加の原因になる過程

カスタマイズしたログ・ソース拡張は、正しく構成されていないと、異常なアセット増加の原因になることがあります。

カスタマイズしたログ・ソース拡張は、中央のログ・サーバーにあるイベント・ペイロードからのユーザー名を解析することで、アセット更新を IBM Security QRadar に提供するように構成します。ログ・ソース拡張は、イベント・ホスト名プロパティーをオーバーライドするように構成します。そうすることで、カスタム・ログ・ソースによって生成されるアセット更新は、必ず中央のログ・サーバーの DNS ホスト名を指定するようになります。

QRadar がユーザーのログイン先のアセットのホスト名を持つ更新を受け取る代わりに、ログ・ソースがすべて同じホスト名を持つアセット更新を多数生成します。

この状態では、異常なアセット増加は、多数の IP アドレスとユーザー名が含まれる 1 つのアセット・プロファイルが原因で発生します。

通常のサイズしきい値を超えるアセット・プロファイルのトラブルシューティング

IBM Security QRadar では、1 つのアセットで累積されるデータがアイデンティティー・データに設定されているしきい値制限を超えると、次のシステム通知が生成されます。

`The system detected asset profiles that exceed the normal size threshold`

説明

通知のペイロードに、最も頻繁に異常が発生する上位 5 件のアセットのリストと、システムで各アセットが異常な増加としてマークされた理由が示されます。次の例に示すように、ペイロードにはアセットがアセット・サイズしきい値を超えて増加しようとした状況の発生回数も示されます。

```
Feb 13 20:13:23 127.0.0.1 [AssetProfilerLogTimer]
com.q1labs.assetprofile.updateresolution.UpdateResolutionManager:
[INFO] [NOT:0010006101][9.21.118.83/- -] [-/- -]
The top five most frequently deviating asset profiles between
Feb 13, 2015 8:10:23 PM AST and Feb 13, 2015 8:13:23 PM AST:
[ASSET ID:1003, REASON:Too Many IPs, COUNT:508],
[ASSET ID:1002, REASON:Too many DNS Names, COUNT:93],
[ASSET ID:1001, REASON:Too many MAC Addresses, COUNT:62]
```

アセット・データが構成されているしきい値を超えると、QRadar はそのアセットのその後の更新をブロックします。この介入により、今後システムが破損データを受信することが防止され、システムが異常に大きなアセット・プロファイルに対して受信した更新を調整しようとする場合に発生するパフォーマンスへの影響を緩和できます。

必要なユーザー処置

通知ペイロードの情報を使用して、異常なアセット増加の原因であるアセットを特定し、異常な増加の原因を判別します。この通知には、過去 24 時間に異常なアセット増加が発生したすべてのアセットのレポートへのリンクが含まれています。

環境内で異常なアセット増加を解決したら、このレポートを再度実行できます。

1. 「ログ・アクティビティー」タブをクリックし、「検索」 > 「新規検索」をクリックします。
2. 「異常なアセット増加**:** アセット・レポート **(Deviating Asset Growth: Asset Report)**」という保存済み検索を選択します。
3. このレポートを使用して、異常発生中に作成された不正確なアセット・データを特定して修復します。

アセット・データが有効な場合、QRadar 管理者は、QRadarの「管理」タブの「アセット・プロファイラー構成」で IP アドレス、MAC アドレス、NetBIOS ホスト名、および DNS ホスト名のしきい値制限を増やすことができます。

関連概念:

285 ページの『失効アセット・データ』
新しいアセット・レコードが作成される割合が、失効アセット・データが削除される割合を超える場合、失効アセット・データが問題となる可能性があります。失効アセット・データが原因で発生する異常なアセット増加に対処する上で重要となるのが、アセット保存しきい値の制御と管理です。

アセット・ブラックリストへの新規アセット・データの追加

アセット・データが異常なアセット増加に一致する振る舞いを示すと、IBM Security QRadar は次のシステム通知を生成します。

```
The asset blacklist rules have added new asset data to the asset blacklists
```

説明

アセット除外ルールは、アセット・データをモニターし、一貫性と整合性を確認します。このルールは一定の期間にわたって特定のアセット・データを追跡し、適切な期間にわたってそのアセット・データが同じデータ・サブセットにより一貫して観測されることを確認します。

例えば、アセット更新に MAC アドレスと DNS ホスト名の両方が含まれている場合、MAC アドレスにはその DNS ホスト名が一定期間にわたって関連付けられています。その MAC アドレスが含まれている後続のアセット更新には、DNS ホスト名が含まれている場合にはその同じ DNS ホスト名も含まれています。突然その MAC アドレスが別の DNS ホスト名に短期間関連付けられた場合、その変更がモニターされます。MAC アドレスが再び短期間にわたって変更されると、その MAC アドレスには、異常なアセット増加の原因となっていることを示すフラグが付けられます。

必要なユーザー処置

通知ペイロードの情報を使用して、アセット・データのモニターに使用されているルールを特定します。通知の「アセットの異常 **(ログ・ソース別) (Asset deviations by log source)**」リンクをクリックして、過去 24 時間に発生したアセットの異常を確認します。

アセット・データが有効な場合は、QRadar 管理者は問題を解決するように QRadar を構成できます。

- ブラックリストへのデータ追加の頻度が高すぎる場合は、ブラックリストにデータを追加するアセット調整除外ルールをチューニングできます。
- アセット・データベースにアセットを追加する場合は、ブラックリストからそのアセット・データを削除し、対応するアセット・ホワイトリストに追加できます。ホワイトリストにアセット・データを追加すると、それらのデータがブラックリストに誤って再び追加されることがなくなります。

関連概念:

295 ページの『アセット調整除外ルールの高度なチューニング』
アセット調整除外ルールをチューニングして、1 つ以上のルールで異常なアセット増加の定義を調整します。

異常なアセット増加の防止

報告されたアセット増加に正当な理由があることを確認した場合は、そのアセットについて IBM Security QRadar が異常なアセット増加のメッセージを起動しないようにする方法がいくつかあります。

異常なアセット増加を防止する方法を決定する上で役立つ情報を次に示します。

- QRadar で失効アセット・データがどのように処理されるかを理解します。
- アセット・プロファイラー保存設定をチューニングして、アセット・データの保存期間の長さを制限します。
- 1 つのアセットに許可される IP アドレスの数をチューニングします。

- アイデンティティー除外検索を作成して、特定のイベントを除外し、それらのイベントからアセット更新が提供されないようにします。
- アセット調整除外ルールをチューニングして、異常なアセット増加の定義を調整します。
- データがアセット・ブラックリストに再び追加されないようにするため、アセット・ホワイトリストを作成します。
- アセット・ブラックリストとアセット・ホワイトリストの項目を変更します。
- DSM が最新であることを確認します。QRadar が提供する週次自動更新には、DSM の更新と解析の問題に対する訂正が含まれていることがあります。

失効アセット・データ

新しいアセット・レコードが作成される割合が、失効アセット・データが削除される割合を超える場合、失効アセット・データが問題となる可能性があります。失効アセット・データが原因で発生する異常なアセット増加に対処する上で重要となるのが、アセット保存しきい値の制御と管理です。

失効アセット・データ とは、特定の期間にわたってアクティブにもパッシブにも監視されていないヒストリカル・アセット・データです。失効アセット・データは、構成されている保存期間を経過すると削除されます。

ヒストリカル・レコードは、IBM Security QRadar によりイベントとフローでパッシブに監視されるか、ポートおよび脆弱性スキャナーでアクティブに監視されると、再びアクティブになります。

異常なアセット増加を防ぐには、1 つのアセットに許可される IP アドレスの数と、QRadar でのアセット・データの保存期間の長さとの適切なバランスを特定する必要があります。高いレベルのアセット・データ保存に対応するように QRadar を構成する前に、パフォーマンスと管理のトレードオフについて検討する必要があります。保存期間を長く設定し、アセットごとのしきい値を高く設定することが常に理想的であるように思われますが、ご使用の環境で対応可能なベースライン構成を特定し、その構成をテストする方が適切です。その後、適切なバランスを得られるまで保存しきい値を少しずつ増加していくことができます。

関連タスク:

291 ページの『アセット・プロファイラー保存設定のチューニング』
IBM Security QRadar は、アセット保存設定を使用してアセット・プロファイルのサイズを管理します。

292 ページの『1 つのアセットに許可される IP アドレスの数の調整』
IBM Security QRadar は、時間の経過に伴い 1 つのアセットに累積される IP アドレスの数をモニターします。

アセット・ブラックリストとアセット・ホワイトリスト

IBM Security QRadar は、アセット調整ルールのグループを使用して、アセット・データが信頼できるかどうかを判別します。アセット・データが疑わしい場合、QRadar は、アセットのブラックリストおよびホワイトリストを使用して、そのアセット・データでアセット・プロファイルを更新するかどうかを判別します。

アセット・ブラックリスト とは、QRadar が信用できないと判断したデータの集合です。アセット・ブラックリストのデータは、異常なアセット増加の原因になる可能性があり、QRadar ではアセット・データベースにこのデータが追加されないようにします。

アセット・ホワイトリスト は、アセット・ブラックリストに追加されるデータに関するアセット調整エンジン・ロジックをオーバーライドする、アセット・データの集合です。システムでは、ブラックリストとの一致が検出されると、ホワイトリストにその値が含まれているかどうかが調べられます。アセット更新がホワイトリストに含まれているデータに一致すると、変更が調整され、アセットが更新されます。ホワイトリストに登録されているアセット・データは、すべてのドメインにグローバルに適用されます。

アセット・ブラックリストとアセット・ホワイトリストはリファレンス・セットです。アセット・ブラックリストとアセット・ホワイトリストを表示および変更するには、QRadar コンソールの「リファレンス・セット管理」ツールを使用します。リファレンス・セットの処理について詳しくは、 171 ページの『リファレンス・セット概要』を参照してください。

あるいは、コマンド・ライン・インターフェース (CLI) または RestFUL API エンドポイントを使用して、アセット・ブラックリストとアセット・ホワイトリストの内容を更新することができます。

アセット・ブラックリスト

アセット・ブラックリスト とは、IBM Security QRadar がアセット調整除外ルールに基づいて信用できないと判断したデータの集合です。アセット・ブラックリストのデータは、異常なアセット増加の原因になる可能性があり、QRadar ではアセット・データベースにこのデータが追加されないようにします。

QRadar でのすべてのアセット更新は、アセット・ブラックリストと比較されます。ブラックリストに登録されたアセット・データは、すべてのドメインにグローバルに適用されます。アセット更新に含まれているアイデンティティー情報 (MAC アドレス、NetBIOS ホスト名、DNS ホスト名、または IP アドレス) がブラックリストで見つかると、受信した更新は破棄され、アセット・データベースは更新されません。

次の表に、各アイデンティティー・アセット・データ・タイプのリファレンス収集名とリファレンス収集タイプを示します。

表 *55.* アセット・ブラックリスト・データのリファレンス収集名

アイデンティティー・データ・タイプ	リファレンス収集名	リファレンス収集タイプ
IP アドレス (v4)	Asset Reconciliation IPv4 Blacklist	リファレンス・セット [セット・タイプ: IP]
DNS ホスト名	Asset Reconciliation DNS Blacklist	リファレンス・セット [セット・タイプ: ALNIC*]
NetBIOS ホスト名	Asset Reconciliation NetBIOS Blacklist	リファレンス・セット [セット・タイプ: ALNIC*]

表 55. アセット・ブラックリスト・データのリファレンス収集名 (続き)

アイデンティティー・データ・タイプ	リファレンス収集名	リファレンス収集タイプ
MAC アドレス	Asset Reconciliation MAC Blacklist	リファレンス・セット [セット・タイプ: ALNIC*]
* ALNIC は、ホスト名と MAC アドレス値の両方に対応する英数字タイプです。		

「リファレンス・セット管理」ツールを使用すると、ブラックリスト項目を編集できます。リファレンス・セットの使用方法については、『リファレンス・セット管理』(http://www.ibm.com/support/knowledgecenter/SS42VS_7.2.7/com.ibm.qradar.doc/c_qradar_adm_mge_ref_set.html) を参照してください。

関連概念:

『アセット・ホワイトリスト』
アセット・ホワイトリストを使用して、IBM Security QRadar アセット・データがアセット・ブラックリストに誤って再び追加されることを防止できます。

アセット・ホワイトリスト

アセット・ホワイトリストを使用して、IBM Security QRadar アセット・データがアセット・ブラックリストに誤って再び追加されることを防止できます。

アセット・ホワイトリスト は、アセット・ブラックリストに追加されるデータに関するアセット調整エンジン・ロジックをオーバーライドする、アセット・データの集合です。システムでは、ブラックリストとの一致が検出されると、ホワイトリストにその値が含まれているかどうかが調べられます。アセット更新がホワイトリストに含まれているデータに一致すると、変更が調整され、アセットが更新されます。ホワイトリストに登録されているアセット・データは、すべてのドメインにグローバルに適用されます。

「リファレンス・セット管理」ツールを使用して、ホワイトリストの項目を編集できます。リファレンス・セットの使用方法については、『リファレンス・セット管理』(http://www.ibm.com/support/knowledgecenter/SS42VS_7.2.7/com.ibm.qradar.doc/c_qradar_adm_mge_ref_set.html) を参照してください。

ホワイトリストの使用例

ホワイトリストは、有効なアセット更新であるにもかかわらずブラックリストに継続的に追加されるアセット・データがある場合に役立ちます。例えば、5 つの IP アドレスのセットを循環するように構成されているラウンドロビン DNS ロード・バランサーがあるとします。アセット調整除外ルールにより、1 つの DNS ホスト名に関連付けられている複数の IP アドレスが、異常なアセット増加を示すものと判断され、この DNS ロード・バランサーがブラックリストに追加されることがあります。この問題を解決するには、この DNS ホスト名を Asset Reconciliation DNS Whitelist に追加します。

アセット・ホワイトリストへの大量入力

正確なアセット・データベースにより、システムで発生したオフェンスをネットワーク上の物理アセットまたは仮想アセットに容易に結び付けることができます。ア

セット・ホワイトリストに大量の項目を追加してアセットの異常を無視することは、正確なアセット・データベースを作成する上では役立ちません。ホワイトリストに大量の項目を追加する代わりに、アセット・ブラックリストを調べ、異常なアセット増加の原因を特定し、その修正方法を決定します。

アセット・ホワイトリストのタイプ

各タイプのアイデンティティー・データはそれぞれ個別のホワイトリストに維持されます。次の表に、各アイデンティティー・アセット・データ・タイプのリファレンス収集名とリファレンス収集タイプを示します。

表 *56.* アセット・ホワイトリスト・データのリファレンス収集名

データのタイプ	リファレンス収集名	リファレンス収集タイプ
IP アドレス	Asset Reconciliation IPv4 Whitelist	リファレンス・セット [セット・タイプ: IP]
DNS ホスト名	Asset Reconciliation DNS Whitelist	リファレンス・セット [セット・タイプ: ALNIC*]
NetBIOS ホスト名	Asset Reconciliation NetBIOS Whitelist	リファレンス・セット [セット・タイプ: ALNIC*]
MAC アドレス	Asset Reconciliation MAC Whitelist	リファレンス・セット [セット・タイプ: ALNIC*]
* ALNIC は、ホスト名と MAC アドレス値に対応する英数字タイプです。		

関連概念:

286 ページの『アセット・ブラックリスト』
アセット・ブラックリスト とは、IBM Security QRadar がアセット調整除外ルールに基づいて信用できないと判断したデータの集合です。アセット・ブラックリストのデータは、異常なアセット増加の原因になる可能性があり、QRadar ではアセット・データベースにこのデータが追加されないようにします。

リファレンス・セット・ユーティリティーを使用したアセット・ブラックリストとアセット・ホワイトリストの更新

IBM Security QRadar リファレンス・セット・ユーティリティーを使用して、アセット・ブラックリストまたはアセット・ホワイトリストで項目を追加または変更できます。

リファレンス・セットを管理するには、QRadar コンソールで `/opt/qradar/bin` から `ReferenceSetUtil.sh` ユーティリティーを実行します。

各リストに新しい値を追加するコマンドを次の表に示します。パラメーター値は、発信元のアセット・データ・ソースにより提供されるアセット更新値と正確に一致している必要があります。

表 57. アセット・ブラックリストおよびアセット・ホワイトリストのデータを変更するコマンド構文

名前	コマンド構文
Asset Reconciliation IPv4 Blacklist	`ReferenceSetUtil.sh add "Asset Reconciliation IPv4 Blacklist"` *IP* 例えば、次のコマンドは IP アドレス 192.168.3.56 をブラックリストに追加します。 `ReferenceSetUtil.sh add "Asset Reconciliation IPv4 Blacklist" 192.168.3.56`
Asset Reconciliation DNS Blacklist	`ReferenceSetUtil.sh add "Asset Reconciliation DNS Blacklist"` *DNS* 例えば、次のコマンドはドメイン名 'misbehaving.asset.company.com' をブラックリストに追加します。 `ReferenceSetUtil.sh add "Asset Reconciliation DNS Blacklist" "misbehaving.asset.company.com"`
Asset Reconciliation NetBIOS Blacklist	`ReferenceSetUtil.sh add "Asset Reconciliation NetBIOS Blacklist"` *NETBIOS* 例えば、次のコマンドは NetBIOS ホスト名 'deviantGrowthAsset-156384' をブラックリストから削除します。 `ReferenceSetUtil.sh delete "Asset Reconciliation NetBIOS Blacklist" "deviantGrowthAsset-156384"`
Asset Reconciliation MAC Blacklist	`ReferenceSetUtil.sh add "Asset Reconciliation MAC Blacklist"` *MACADDR* 例えば、次のコマンドは MAC アドレス '00:a0:6b:54:9f:0e' をブラックリストに追加します。 `ReferenceSetUtil.sh add "Asset Reconciliation MAC Blacklist" "00:a0:6b:54:9f:0e"`
Asset Reconciliation IPv4 Whitelist	`ReferenceSetUtil.sh add "Asset Reconciliation IPv4 Whitelist"` *IP* 例えば、次のコマンドは IP アドレス 10.1.95.142 をホワイトリストから削除します。 `ReferenceSetUtil.sh delete "Asset Reconciliation IPv4 Whitelist" 10.1.95.142`
Asset Reconciliation DNS Whitelist	`ReferenceSetUtil.sh add "Asset Reconciliation DNS Whitelist"` *DNS* 例えば、次のコマンドはドメイン名 'loadbalancer.company.com' をホワイトリストに追加します。 `ReferenceSetUtil.sh add "Asset Reconciliation DNS Whitelist" "loadbalancer.company.com"`

表 57. アセット・ブラックリストおよびアセット・ホワイトリストのデータを変更するコマンド構文 (続き)

名前	コマンド構文

Asset Reconciliation NetBIOS Whitelist	`ReferenceSetUtil.sh add "Asset Reconciliation NetBIOS Whitelist" NETBIOS`
	
	例えば、次のコマンドは NetBIOS 名 'assetName-156384' をホワイトリストに追加します。
	
	`ReferenceSetUtil.sh add "Asset Reconciliation NetBIOS Whitelist" "assetName-156384"`

Asset Reconciliation MAC Whitelist	`ReferenceSetUtil.sh add "Asset Reconciliation MAC Blacklist" MACADDR`
	
	例えば、次のコマンドは MAC アドレス '00:a0:6b:54:9f:0e' をブラックリストに追加します。
	
	`ReferenceSetUtil.sh add "Asset Reconciliation MAC Blacklist" "00:a0:6b:54:9f:0e"`

関連タスク:

『RESTful API を使用したブラックリストとホワイトリストの更新』
IBM Security QRadar RESTful API を使用して、アセットのブラックリストとホワイトリストの内容をカスタマイズできます。

RESTful API を使用したブラックリストとホワイトリストの更新

IBM Security QRadar RESTful API を使用して、アセットのブラックリストとホワイトリストの内容をカスタマイズできます。

このタスクについて

表示または更新するリファレンス・セットの正確な名前を指定する必要があります。

- Asset Reconciliation IPv4 Blacklist
- Asset Reconciliation DNS Blacklist
- Asset Reconciliation NetBIOS Blacklist
- Asset Reconciliation MAC Blacklist
- Asset Reconciliation IPv4 Whitelist
- Asset Reconciliation DNS Whitelist
- Asset Reconciliation NetBIOS Whitelist
- Asset Reconciliation MAC Whitelist

手順

1. Web ブラウザーに次の URL を入力し、RESTful API インターフェースにアクセスします。

   `https://ConsoleIPaddress/api_doc`

2. 左側のナビゲーション・ペインで 4.0>/reference_data >/sets > /{name} を見つけます。
3. アセット・ブラックリストまたはアセット・ホワイトリストの内容を確認するには、次の手順を実行します。
   a. 「**GET**」タブをクリックし、「パラメーター」セクションまでスクロールダウンします。
   b. 「名前」パラメーターの「値」フィールドに、表示するアセット・ブラックリストまたはアセット・ホワイトリストの名前を入力します。
   c. 「試用」をクリックし、画面下部に表示される結果を確認します。
4. アセット・ブラックリストまたはアセット・ホワイトリストに値を追加するには、次の手順を実行します。
   a. 「**POST**」タブをクリックし、「パラメーター」セクションまでスクロールダウンします。
   b. 次のパラメーターの値を入力します。

表 *58.* 新規アセット・データを追加するために必要なパラメーター

パラメーター名	パラメーターの説明
name	更新するリファレンス収集の名前を示します。
value	アセット・ブラックリストまたはアセット・ホワイトリストに追加するデータ項目を示します。発信元のアセット・データ・ソースから提供されるアセット更新値と正確に一致している必要があります。

   c. 「試用」をクリックして、新しい値をアセット・ホワイトリストまたはアセット・ブラックリストに追加します。

次のタスク

RESTful API を使用したリファレンス・セットの変更について詳しくは、「*IBM Security QRadar API ガイド*」を参照してください。

関連概念:

288 ページの『リファレンス・セット・ユーティリティーを使用したアセット・ブラックリストとアセット・ホワイトリストの更新』

IBM Security QRadar リファレンス・セット・ユーティリティーを使用して、アセット・ブラックリストまたはアセット・ホワイトリストで項目を追加または変更できます。

アセット・プロファイラー保存設定のチューニング

IBM Security QRadar は、アセット保存設定を使用してアセット・プロファイルのサイズを管理します。

ほとんどのアセット・データのデフォルト保存期間は、QRadar で最後にアクティブまたはパッシブに監視された時点から 120 日です。ユーザー名の保存期間は 30 日です。

通常、QRadar ユーザーが手動で追加したアセット・データは、異常なアセット増加の原因となることはありません。デフォルトでは、このデータは永久に保存されます。その他のタイプのアセット・データの場合、静的環境でのみ「永久保存」フラグを設定することが推奨されます。

このタスクについて

イベント内のアセット・アイデンティティー・データのタイプに応じて保存期間を調整できます。例えば複数の IP アドレスが 1 つのアセットにマージされている場合、IP 保存期間を 120 日からこれよりも短い値に変更できます。

特定のタイプのアセット・データのアセット保存期間を変更すると、QRadar 内のすべてのアセット・データに新しい保存期間が適用されます。既存のアセット・データが新しいしきい値をすでに超えている場合、デプロイメントの完了時にこのアセット・データは削除されます。アセット・データが保存期間を経過している場合でも常に指定されたホストを識別できるようにするため、アセット保存クリーンアップ・プロセスでは、アセットの最後に認識されたホスト名値は削除されません。

アセット・データの保存日数を決定する前に、長い保存期間に関する次の特徴を理解しておいてください。

- アセットのヒストリカル・ビューが向上します。
- アセット・データベース内に作成されるアセットあたりのデータ・ボリュームが大きくなります。
- 失効データが原因で異常なアセット増加が発生する確率が高くなります。

手順

1. 「管理」タブをクリックします。
2. ナビゲーション・メニューで、「システム構成」をクリックします。
3. 「アセット・プロファイラー構成」をクリックします。
4. 「アセット・プロファイラーの保存構成」をクリックします。
5. 保存値を調整して「保存」をクリックします。
6. 更新を反映するため、変更内容を環境にデプロイします。

関連タスク:

『1 つのアセットに許可される IP アドレスの数の調整』
IBM Security QRadar は、時間の経過に伴い 1 つのアセットに累積される IP アドレスの数をモニターします。

1 つのアセットに許可される IP アドレスの数の調整

IBM Security QRadar は、時間の経過に伴い 1 つのアセットに累積される IP アドレスの数をモニターします。

デフォルトでは、1 つのアセットに累積される IP アドレスの数が 75 を超えると、QRadar によりシステム・メッセージが生成されます。アセットに累積される IP アドレスの数が 75 を超えると予想される場合は、「**1** つのアセットに許可される **IP** の数」の値を調整して、システム・メッセージが今後表示されないようにすることができます。

このタスクについて

IP アドレス数制限の設定値が大きすぎると、QRadar が、デプロイメントの他の部分へ悪影響を及ぼす前に、異常なアセット増加を検出できなくなります。この制限の設定値が小さすぎると、報告される異常なアセット増加の数が増加します。

初めて「**1** つのアセットに許可される **IP** の数」の値を調整するときには、次のガイドラインを使用できます。

1 つのアセットに許可される IP アドレスの数 = (<保存期間 *(*日数*)*> x *<1* 日あたりの *IP* アドレスの推定数>) + *<IP* アドレスのバッファー数>

各部分の説明は次のとおりです。

- *<1* 日あたりの *IP* アドレスの推定数> は、通常の条件下で 1 日あたりに 1 つのアセットに累積される IP アドレスの数です。
- <保存期間 *(*日数*)*> は、アセットの IP アドレスの保存期間です。

手順

1. 「管理」タブをクリックします。
2. ナビゲーション・メニューで、「システム構成」をクリックします。
3. 「アセット・プロファイラー構成」をクリックします。
4. 「アセット・プロファイラーの保存構成」をクリックします。
5. 構成値を調整して「保存」をクリックします。
6. 更新を反映するため、変更内容を環境にデプロイします。

関連タスク:

291 ページの『アセット・プロファイラー保存設定のチューニング』
IBM Security QRadar は、アセット保存設定を使用してアセット・プロファイルのサイズを管理します。

アイデンティティー除外検索

アイデンティティー除外検索を使用して、判明している妥当な理由で大量の類似するアイデンティティー情報が累積される単一アセットを管理できます。

例えば、ログ・ソースから大量のアイデンティティー情報がアセット・データベースに提供されることがあります。ほぼリアルタイムでのアセット情報の変更が IBM Security QRadar に提供され、アセット・データベースに最新の内容が維持されます。ただしログ・ソースは、ほとんどの場合に、異常なアセット増加やその他のアセット関連の異常な状況の原因となります。

ログ・ソースから QRadar に誤ったアセット・データが送信される場合は、アセット・データベースで有効なデータが送信されるように、ログ・ソースを修正してください。ログ・ソースを修正できない場合は、アセット・データベースへのアセット情報の入力をブロックするアイデンティティー除外検索を作成できます。

また、`Identity_Username+Is Any Of + Anonymous Logon` が指定されているアイデンティティー除外検索を使用して、サービス・アカウントや自動サービスに関連するアセットを更新しないようにすることもできます。

アイデンティティー除外検索とブラックリストの相違点

アイデンティティー除外検索は、機能の点でアセット・ブラックリストに類似しているように見えますが、大きく異なる点があります。

ブラックリストには、除外対象の生アセット・データ (MAC アドレス、ホスト名など) のみを指定できます。アイデンティティー除外検索では、ログ・ソース、カテゴリー、イベント名などの検索フィールドに基づいて、アセット・データがフィルタリングされます。

ブラックリストでは、データを提供するデータ・ソースのタイプは考慮されませんが、アイデンティティー除外検索はイベントにのみ適用できます。アイデンティティー除外検索では、一般的なイベント検索フィールド (イベント・タイプ、イベント名、カテゴリー、ログ・ソースなど)に基づいてアセット更新をブロックできます。

アイデンティティー除外検索の作成

特定のイベントを除外し、これらのイベントからアセット・データベースにアセット・データが提供されないようにするために、IBM Security QRadar アイデンティティー除外検索を作成できます。

このタスクについて

この検索用に作成するフィルターは、維持するイベントではなく除外するイベントに一致する必要があります。

既にシステム内にあるイベントに対してこの検索を実行すると便利です。ただしこの検索を保存するときには、「タイム・スパン」オプションで「リアルタイム **(**ストリーミング**)**」を選択する必要があります。この設定を選択しないと、QRadar が受信するイベントのライブ・ストリームに対してこの検索を実行するときに、一致する結果がありません。

保存したアイデンティティー除外検索を更新し、名前を変更しないと、アセット・プロファイラーにより使用されるアイデンティティー除外リストが更新されます。例えば、検索を編集して、除外するアセット・データのフィルター操作を追加するとします。新しい値が追加され、検索保存直後にアセット除外が開始されます。

手順

1. 「ログ・アクティビティー」タブで「検索」 > 「新規検索」をクリックします。
2. アセット更新から除外するイベントを突き合わせる検索条件とフィルターを追加して検索を作成します。
3. 「時刻範囲」ボックスで「リアルタイム **(**ストリーミング**)**」を選択し、「フィルター」をクリックして検索を実行します。
4. 検索結果画面で「条件の保存」をクリックし、保存する検索の情報を入力します。 保存済み検索を検索グループに割り当てることができます。アイデンティティー除外検索グループは、「認証、アイデンティティー、およびユーザーのアクティビティー」フォルダー内にあります。

「タイム・スパン」オプションで「リアルタイム **(**ストリーミング**)**」が選択されていることを確認します。

5. 「**OK**」をクリックして検索を保存します。
6. 「管理」タブをクリックし、「アセット・プロファイラー構成」をクリックします。
7. 画面下部で「アイデンティティーの除外の管理」をクリックします。
8. 左側の検索リストから、作成したアイデンティティー除外検索を選択し、追加アイコン (>) をクリックします。 検索が見つからない場合は、リスト上部のフィルターに先頭の数文字を入力します。
9. 「保存」をクリックします。
10. 更新を反映するため、変更内容を環境にデプロイします。

アセット調整除外ルールの高度なチューニング

アセット調整除外ルールをチューニングして、1 つ以上のルールで異常なアセット増加の定義を調整します。

アセット調整除外ルールの次の正規化テンプレートを例に説明します。

```
Apply AssetExclusion: Exclude DNS Name By IP on events which are detected
 by the Local system and NOT when any of
Identity Host Name are contained in any of
Asset Reconciliation DNS Whitelist - AlphaNumeric (Ignore Case),
 Asset Reconciliation DNS Blacklist - AlphaNumeric (Ignore Case)
 and when at least N1 events are seen with the same
Identity Host Name and different Identity IP in N2
```

次の表に、このルール・テンプレートでチューニング可能な変数と変更結果を示します。テンプレートのその他の変数は変更しないでください。

表 *59.* アセット調整ルールのチューニングのオプション

変数	デフォルト値	チューニング結果
N1	3	この変数を低い値にチューニングすると、ブラックリストに追加されるデータが増加します。これは、このルールを起動するために必要な、競合データを含むイベントの数が少なくなるためです。 この変数を高い値にチューニングすると、ブラックリストに追加されるデータが減少します。これは、このルールを起動するために必要な、競合データを含むイベントの数が増加するためです。

表 59. アセット調整ルールのチューニングのオプション (続き)

変数	デフォルト値	チューニング結果
N2	2 時間	この変数を低い値にチューニングすると、このルールが起動するために必要な、N1 個のイベントが発生する必要がある時間が短くなります。一致データを監視する必要がある時間が短くなり、その結果ブラックリストに追加されるデータが減少します。 この変数を高い値にチューニングすると、このルールが起動するために必要な、N1 個のイベントが発生する必要がある時間が長くなります。一致データを監視する時間が長くなり、その結果ブラックリストに追加されるデータが増加します。 この期間を長くすると、データが追跡される期間が長くなるため、システム・メモリー・リソースに影響を及ぼす可能性があります。

アセット調整除外ルールはシステム全体に適用されるルールです。このルールを変更すると、システム全体におけるこのルールの動作に影響します。

ルールへのさまざまなチューニングの適用

場合によっては、システムのさまざまな部分でルールに異なるチューニングを適用する必要があります。ルールに異なるチューニングを適用するには、チューニングするアセット調整除外ルールのコピーを作成し、システムの特定部分のみをテストするようにルールを制限するためテストを 1 つ以上追加します。例えば、ネットワーク、ログ・ソース、またはイベント・タイプのみをテストするルールを作成できます。

このタスクについて

一部のタスクや CRE ルールはシステム・パフォーマンスに影響するため、システムに新しいルールを追加するときには常に注意してください。アセット更新が新しいルールの条件に一致した場合は常にシステムでそれ以降のテスト・ロジックをバイパスできるように、各テスト・スタックの先頭に新しいルールを追加すると効果的です。

手順

1. ルールのコピーを作成します。
   a. 「オフェンス」タブで「ルール」をクリックし、コピーするルールを選択します。
   b. 「アクション」 > 「コピー」をクリックします。 新しいルールに、ルールをコピーする理由を示す名前を付けると便利です。
2. ルールにテストを追加します。

   ルールをシステム・データのサブセットにのみ適用するために使用するフィルターを決定します。例えば、特定のログ・ソースからのイベントのみを突き合わせるテストを追加できます。
3. 必要な動作が実現するように、ルールの変数をチューニングします。
4. 元のルールを更新します。

a. コピーのルールに追加したテストを元のルールに追加します。ただし、ルールの AND 演算子と AND NOT 演算子を逆にします。

   演算子を逆にすると、両方のルールでイベントがトリガーされることを防止できます。

例: ブラックリストから IP アドレスを除外するようにチューニングされたアセット除外ルール

アセット除外ルールをチューニングして、IP アドレスがブラックリストに登録されないように除外することができます。

ネットワーク・セキュリティー管理者であるあなたは、通常は短期である IP アドレス・リースが頻繁に発生する公衆 WiFi ネットワーク・セグメントが含まれる企業ネットワークを管理しています。このネットワーク・セグメントのアセットは一時的なものである傾向にあります (主に公衆 WiFi に頻繁にログイン/ログアウトするハンドヘルド・デバイスとノートブックです)。一般に、短期間のうちに 1 つの IP アドレスが複数デバイスによって複数回使用されます。

デプロイメントのその他の部分には、インベントリーに登録されており、適切な名前が設定された社内デバイスのみで構成され、慎重に管理されているネットワークがあります。このネットワーク部分の IP アドレス・リースはかなり長く、IP アドレスへのアクセスは認証によってのみ行われます。このネットワーク・セグメントで、異常なアセット増加が発生したことを即時に把握し、アセット調整除外ルールのデフォルト設定を維持することを望んでいます。

ブラックリストへの IP アドレスの登録

この環境では、デフォルトのアセット調整除外ルールによって短期間のうちにネットワーク全体が誤ってブラックリストに登録されます。

セキュリティー・チームは、WiFi セグメントによって生成されるアセット関連の通知が不適切であると判断しました。今後 WiFi から異常なアセット増加に関する通知がトリガーされないようにします。

アセット調整ルールのチューニングによる一部のアセット更新の無視

最後のシステム通知で「ログ・ソース別アセット異常 **(Asset deviation by log source)**」レポートを確認します。ブラックリストに登録されたデータが、WiFi の DHCP サーバーから送信されたものであることが判明しました。

「**AssetExclusion: Exclude IP By MAC Address**」ルールに対応する行の「イベント数」列、「フロー数」列、および「オフェンス数」列の値は、WiFi DHCP サーバーによってこのルールがトリガーされたことを示しています

既存のアセット調整除外ルールに、ルールによるブラックリストへの WiFi データの追加を防止するためのテストを追加します。

```
Apply AssetExclusion:Exclude IP by MAC address on events which are detected by
the Local system and NOT when the event(s) were detected by one or more of
MicrosoftDHCP @ microsoft.dhcp.test.com
and NOT when any of Domain is the key and any of Identity IP is the value in
```

```
any of Asset Reconciliation Domain IPv4 Whitelist
- IP Asset Reconciliation Domain IPv4 Blacklist - IP
and when at least 3 events are seen with the same Identity IP and
different Identity MAC in 2 hours.
```

更新されたルールは、WiFi DHCP サーバー上にないログ・ソースからのイベントだけをテストします。WiFi DHCP イベントがより高負荷のリファレンス・セットおよび動作分析テストを実行しないようにするには、このテストをテスト・スタックの先頭に移動します。

異常増加後のアセット・データのクリーンアップ

IBM Security QRadar はアセット・モデルを使用して、デプロイメント内のオフェンスをネットワーク上の物理アセットまたは仮想アセットに結び付けます。セキュリティーの問題を解決するときには、アセットの使用状況に関連したデータを収集して表示できることが不可欠です。データを最新かつ正確な状態に保つには、アセット・データベースの保守が重要です。

問題の原因を修正する場合でも、アセット更新をブロックする場合でも、無効なアセット・データを削除し、アセット・ブラックリストの項目を削除することで、アセット・データベースをクリーンアップする必要があります。

無効なアセットの削除

異常なアセット増加の原因であるアセットを修正したら、選択式クリーンアップを使用するか、またはアセット・データベースを再作成して、アセット成果物をクリーンアップします。

このタスクについて

選択式クリーンアップ
: これは、限られた範囲の異常なアセット増加の場合の方法です。影響を受けたアセットを選択して削除する方法は、アセット成果物を最も安全にクリーンアップできますが、多数のアセットが影響を受けている場合は非常に煩雑な操作となることもあります。

アセット・データベースの再作成
: アセット・データベースを新規に再作成する方法は、異常なアセット増加が広範囲にわたる場合に最も効率的かつ正確なアセット削除方法です。

  この方法では、アセット増加の問題を解決するために構成した新しいチューニングに基づいて、データベースでパッシブにアセットを再生成します。この方法では、すべてのスキャン結果と残っているアセット・データが失われますが、スキャンを再実行するか、スキャン結果を再インポートすることでこのデータを取り戻すことができます。

手順

1. アセット・データベースで無効な成果物を選択して削除するには、次の手順を実行します。
   a. 「ログ・アクティビティー」タブで「異常なアセット増加**:** アセット・レポート **(Deviating Asset Growth: Asset Report)**」というイベント検索を実

行します。 この検索では、異常なアセット増加の影響を受け、削除する必要があるアセットのレポートが返されます。

b. 「アセット」タブで「アクション」 > 「アセットの削除」をクリックします。 アセットが IBM Security QRadar で非表示になるまでに遅延が生じることがあります。

2. アセット・データベースを新規に再作成するには、次の手順を実行します。

a. SSH を使用して QRadar コンソールに管理者としてログインします。

b. コンソール・コマンド・ラインから `/opt/qradar/support/cleanAssetModel.sh` スクリプトを実行し、プロンプトが表示されたら「オプション **1 (Option 1)**」を選択します。

アセット・データベースを再作成すると、アセット調整エンジンが再始動されます。

タスクの結果

ブラックリストをパージすると、手動で追加された項目を含むすべてのブラックリスト項目が削除されます。手動で追加したブラックリスト項目は、再度手動で追加する必要があります。

ブラックリスト項目の削除

ブラックリスト項目の原因を修正したら、ブラックリストにある該当項目をクリーンアップする必要があります。個々のブラックリスト項目を削除できますが、ブラックリストのすべての項目をパージし、異常なアセット増加に関連しないブラックリスト値を再生成できるようにする方法をお勧めします。

手順

1. IBM Security QRadar コンソールを使用してブラックリストをパージするには、次の手順を実行します。

a. 「管理」 > 「システム構成」 > 「リファレンス・セット管理」をクリックします。

b. リファレンス・セットを選択して「削除」をクリックします。

c. クイック検索テキスト・ボックスを使用して、削除するリファレンス・セットを検索し、「リスト内容の削除」をクリックします。

2. QRadar コンソール コマンド・ライン・インターフェースを使用してブラックリストをパージするには、次の手順を実行します。

a. `/opt/qradar/bin` ディレクトリーに移動します。

b. 次のコマンドを実行します。

```
./ReferenceDataUtil.sh purge "Reference Collection Name"
```

ここで *Reference Collection Name* は次のいずれかのリストです。

- Asset Reconciliation NetBIOS Blacklist
- Asset Reconciliation DNS Blacklist
- Asset Reconciliation IPv4 Blacklist
- Asset Reconciliation MAC Blacklist

タスクの結果

ブラックリストをパージすると、手動で追加された項目を含むすべてのブラックリスト項目が削除されます。手動で追加したブラックリスト項目は、再度手動で追加する必要があります。

第 19 章 データを別のシステムに転送するための QRadar システムの構成

IBM Security QRadar システムを構成して、データを 1 つ以上のベンダー・システム (チケット・システムやアラート・システムなど) に転送できます。正規化されたデータを他の QRadar システムに転送することもできます。QRadar からデータを受け取るターゲット・システムを、「宛先転送」と呼びます。

ドメインのタグ付けを除き、QRadar システムはすべてのデータを変更せずに転送します。ドメイン情報は転送データから削除されます。ドメイン情報が含まれているイベントおよびフローは、受信側のシステム上のデフォルト・ドメインに自動的に割り当てられます。

イベントおよびフロー・データの送信時に互換性の問題が発生するのを防ぐため、データを受信するデプロイメント環境が、データを送信するデプロイメント環境と同じバージョンか、それ以上のバージョンになっていることを確認してください。

1. 1 つ以上の宛先転送を構成します。
2. 転送するデータを決定するために、ルーティング・ルールかカスタム・ルール、またはその両方を構成します。
3. データに適用するルーティング・オプションを構成します。

例えば、特定のチケット・システムに転送するように、特定のイベント・コレクターからすべてのデータを構成できます。ルーティング・ルールに一致するデータを削除することによって、相関をバイパスすることもできます。

関連概念:

5 ページの『IBM Security QRadar 製品の機能』
IBM Security QRadar 製品資料では、オフェンス、フロー、アセット、ヒストリカル相関などの機能について説明していますが、すべての QRadar 製品でこれらの機能を利用できるわけではありません。使用する製品によっては、説明されている一部の機能をデプロイメントで使用できない場合があります。各製品の機能を確認して、必要な情報を入手してください。

宛先転送の追加

一括または選択的なデータ転送を構成するには、宛先転送を追加する必要があります。

手順

1. 「管理」タブをクリックします。
2. ナビゲーション・ペインで、「システム構成」をクリックします。
3. 「宛先転送」アイコンをクリックします。
4. ツールバーで、「追加」をクリックします。
5. 「宛先転送」ウィンドウで、パラメーターの値を入力します。

以下の表に、いくつかの「宛先転送」パラメーターを示します。

表 60. 「宛先転送」パラメーター

パラメーター	説明
イベント・フォーマット	• 「ペイロード」は、ログ・ソースまたはフロー・ソースが送信される形式のデータです。 • 「正規化済み」は、ユーザー・インターフェース用の判読可能な情報として解析および準備された生データです。
宛先アドレス	データの転送先となるベンダー・システムの IP アドレスまたはホスト名。
プロトコル	正規化されたデータを TCP プロトコルを使用して送信するには、「**TCP**」プロトコルを使用します。ポート 32004 上の宛先アドレスにオフサイト・ソースを作成する必要があります。
syslog ヘッダーが欠落しているか無効な場合に、syslog ヘッダーを前に付加する	有効な syslog ヘッダーが元の syslog メッセージで検出されず、このチェック・ボックスが選択されている場合、前に付加される syslog ヘッダーの「ホスト名」フィールドには、IBM Security QRadar が受信したパケットの送信元 IP アドレスが含められます。このチェック・ボックスを選択しなかった場合は、変更されていないデータが送信されます。 QRadar が syslog メッセージを転送するときに、アウトバウンド・メッセージが検証され、有効な syslog ヘッダーを持っていることが確認されます。

6. 「保存」をクリックします。

転送プロファイルの構成

宛先転送に転送するプロパティーを指定する場合は、転送プロファイルを構成します。

IBM Security QRadar V7.2.3 以前で作成した JSON 転送プロファイルを再作成する必要があります。

このタスクについて

転送プロファイルを使用できるのは、イベント・データが JSON 形式で送信される場合のみです。

外部の宛先に転送する場合は、特定のイベント・プロパティーやフロー・プロパティー (カスタム・プロパティーを含む) を選択することができます。属性の別名とデフォルト値を指定すると、イベント・データを簡単に識別することができます。プロファイル内で停止されている別名とデフォルト値は、そのプロファイル固有の値になります。別名とデフォルト値を持つ属性を別のプロファイルで使用する場合は、それらの別名とデフォルト値を定義し直す必要があります。

1 つのプロファイルで複数の宛先転送を指定できます。プロファイルを編集する場合は、そのプロファイルが関連付けられているすべての宛先転送について、適切に編集する必要があります。

プロファイルを削除すると、そのプロファイルを使用していたすべての宛先転送で、自動的にデフォルトのプロファイルが使用されるようになります。

手順

1. 「管理」タブをクリックし、ナビゲーション・ペインで「システム構成」をクリックします。
2. 「宛先転送」アイコンをクリックします。
3. ツールバーで「プロファイル・マネージャー」をクリックします。
4. 新しいプロファイルを作成する場合は、「新規」をクリックします。
5. 次に、プロファイルの名前を入力し、イベント・データ・セットに含める属性の横に表示されているチェック・ボックスを選択します。
6. 既存のプロファイルを変更する場合は、対象のプロファイルを選択して「編集」または「削除」をクリックします。
7. 「保存」をクリックします。

一括転送用ルーティング・ルールの構成

1 つ以上の宛先転送を追加したら、フィルター・ベースのルーティング・ルールを作成することで、大容量のデータを転送できるようになります。

このタスクについて

データ転送のためのルーティング・ルールは、以下に示すとおり、オンライン・モードにもオフライン・モードにも構成できます。

- 「オンライン **(Online)**」モードでは、転送がリアルタイムで実行されるため、データは最新の状態に保たれます。宛先転送が到達不能になった場合、データが失われる可能性があります。
- 「オフライン」モードでは、すべてのデータはいったんデータベースに格納されてから宛先転送に送信されます。これにより、データが失われることはなくなりますが、データ転送に遅延が生じることがあります。

以下の表で、「ルーティング・ルール」パラメーターの一部について説明します。

表 *61.* 「ルーティング・ルール」ウィンドウのパラメーター

パラメーター	説明
転送イベント・コレクター (Forwarding Event Collector)	このオプションは、「オンライン **(Online)**」オプションを選択すると表示されます。 このルーティング・ルールでデータを処理するイベント・コレクターを指定します。
転送イベント・プロセッサー・プログラム (Forwarding Event Processor)	このオプションは、「オフライン」オプションを選択すると表示されます。 このルーティング・ルールでデータを処理するイベント・プロセッサーを指定します。 **制約事項:** 「ルーティング・オプション」ペインで「除去」が選択されている場合、このオプションは使用不可です。

表 61. 「ルーティング・ルール」ウィンドウのパラメーター (続き)

パラメーター	説明
ルーティング・オプション	• 「転送」オプションは、データを指定の宛先転送に転送することを指定します。データはデータベースにも保存され、カスタム・ルール・エンジン (CRE) によって処理されます。 • 「除去」オプションは、データが除去されることを示します。データはデータベースに保管されず、CRE によって処理されません。このオプションは、「オフライン」オプションが選択されている場合は使用不可です。 • 「バイパス相関」オプションは、データが CRE をバイパスするが、データベースに保管されることを指定します。このオプションは、「オフライン」オプションが選択されている場合は使用不可です。 2 つのオプションを結合できます。 • 「転送」および「除去」 データは、指定の宛先転送に転送されます。データはデータベースに保管されず、CRE によって処理されません。 • 「転送」および「バイパス相関」 データは、指定の宛先転送に転送されます。データはデータベースにも保存されますが、CRE によって処理されません。転送宛先にある CRE がデータを処理します。 データが複数のルールに一致する場合、最も安全なルーティング・オプションが適用されます。例えば、ドロップするよう構成されたルールと CRE 処理をバイパスするルールとにデータが一致する場合、そのデータはドロップされません。代わりに、データは CRE をバイパスして、データベースに保存されます。 ドロップされるイベントは、60% のレートで EPS ライセンスに返され、すべてのログ・ソースで最大 2000 イベントになります。

手順

1. 「管理」タブをクリックします。
2. ナビゲーション・ペインで、「システム構成」をクリックします。
3. 「ルーティング・ルール」アイコンをクリックします。

4. ツールバーで、「追加」をクリックします。
5. 「ルーティング・ルール」ウィンドウで、パラメーターの値を入力します。
   a. ルーティング・ルールの名前および説明を入力します。
   b. 「モード」フィールドで、「オンライン **(Online)**」か「オフライン」のオプションからいずれか 1 つを選択します。
   c. 「転送イベント・コレクター」リストまたは「イベント・プロセッサーの転送中」リストから、データの転送元とするイベント・コレクターを選択します。
   d. 「イベント・フィルター」セクションの「データ・ソース」フィールドで、経路指定するデータ・ソースとして、「イベント」か「フロー」のいずれかを選択します。

      「フロー・フィルター」オプションを選択した場合、セクション・タイトルは「フロー・フィルター」に変わり、また「すべての受信イベントの突き合わせ」チェック・ボックスは「すべてのフローの突き合わせ」に変わります。
   e. すべての受信データを転送するために、「すべての受信イベントの突き合わせ」または「すべての受信フローの突き合わせ **(Match All Incoming Flows)**」チェック・ボックスを選択します。

      制約事項**:** このチェック・ボックスを選択する場合、フィルターを追加することはできません。
   f. フィルターを追加するために、「イベント・フィルター」または「フロー・フィルター」セクションで、1 番目のリストからフィルターを、2 番目のリストからオペランドを選択します。
   g. テキスト・ボックスに、フィルターに適用する値を入力してから「フィルターの追加」をクリックします。
   h. 追加するフィルターごとに、上記の 2 つのステップを繰り返します。
   i. 現在のフィルターと一致するログ・データを転送するために、「転送」チェック・ボックスを選択してから、使用する宛先転送ごとにチェック・ボックスを選択します。

      制約事項**:** 「転送」チェック・ボックスを選択すると、「除去」または「バイパス相関」チェック・ボックスのいずれかを選択できますが、両方を選択することはできません。

      宛先転送を編集、追加、または削除する場合は、「宛先の管理」リンクをクリックします。
6. 「保存」をクリックします。

選択式転送の構成

「カスタム・ルール」ウィザードを使用して、高度な選択式イベント・データ転送を構成します。ルールの応答として 1 つ以上の宛先転送にイベント・データが転送されるようルールを構成します。

このタスクについて

宛先転送に転送されるイベント・データを決定する基準は、ルールに含まれているテストとビルディング・ブロックに基づいています。ルールが構成および有効化されると、ルール・テストに一致するすべてのイベント・データは、指定された宛先転送に自動的に送信されます。ルールを編集または追加する方法について詳しくは、製品の「*IBM Security QRadar* ユーザー・ガイド」を参照してください。

手順

1. 「オフェンス」 「ログ・アクティビティー」タブをクリックします。
2. ナビゲーション・メニューで、「ルール」を選択します。
3. ルールを編集または追加する。「ルール」ウィザードの「ルールの応答」ページで、「宛先転送に送信」オプションが選択されているようにします。

宛先転送の表示

「宛先転送」ウィンドウには、宛先転送に関する有用な情報が含まれています。各宛先転送に送信されたデータについての統計が表示されます。

例えば、次の情報を確認できます。

- この宛先転送に対して出現したイベントとフローの合計数。
- この宛先転送に送信されたイベントまたはフローの数。
- この宛先転送に到達する前にドロップされたイベントまたはフローの数。

手順

1. 「管理」タブをクリックします。
2. ナビゲーション・メニューで、「システム構成」をクリックします。
3. 「宛先転送」アイコンをクリックします。
4. 宛先転送の統計が表示されます。

宛先転送の表示と管理

「宛先転送」ウィンドウを使用して、宛先転送を表示、編集、および削除します。

手順

1. 「管理」タブをクリックします。
2. ナビゲーション・ペインで、「システム構成」をクリックします。
3. 「宛先転送」アイコンをクリックします。

   各宛先転送に送信されたデータについての統計が表示されます。例えば、次の情報を確認できます。

   - この宛先転送に対して出現したイベントとフローの合計数。
   - この宛先転送に送信されたイベントまたはフローの数。
   - この宛先転送に到達する前にドロップされたイベントまたはフローの数。
4. ツールバーで、以下の表で説明されているとおりに、アクションをクリックします。

表 62. 「宛先転送」ツールバーのアクションについての説明

アクション	説明
カウンターのリセット **(Reset Counters)**	「出現」、「送信」、および「ドロップ」の各パラメーターのカウンターをゼロにリセットします。カウンターは再度集計を開始します。 **ヒント:** カウンターをリセットすると、宛先転送のパフォーマンスについて、対象をより絞り込んで表示することができます。
編集	構成名、フォーマット、IP アドレス、ポート、またはプロトコルを変更します。
削除	宛先転送の削除 宛先転送が有効なルールに関連付けられている場合、宛先転送を削除することを確認する必要があります。

ルーティング・ルールの表示と管理

「イベント・ルーティング・ルール」ウィンドウには、ルーティング・ルールに関する有用な情報が含まれています。データが各ルールに一致する場合の、構成済みのフィルターおよびアクションを表示および管理することができます。

ルールを編集、有効化、無効化、または削除するには、「イベント・ルーティング・ルール (Event Routing Rules)」ウィンドウを使用します。ルーティング・ルールを編集して、構成名、イベント・コレクター、フィルターまたはルーティング・オプションを変更できます。

手順

1. 「管理」タブをクリックします。
2. ナビゲーション・メニューで、「システム構成」をクリックします。
3. 「ルーティング・ルール」アイコンをクリックします。
4. 管理するルーティング・ルールを選択します。
5. ルーティング・ルールを編集するには、ツールバーで「編集」をクリックし、パラメーターを更新します。
6. ルーティング・ルールを削除するには、ツールバーで「削除」をクリックします。
7. ルーティング・ルールを有効化または無効化するには、ツールバーで「有効化/無効化」をクリックします。

   イベントをドロップするよう構成されたルーティング・ルールを有効にすると、確認メッセージが表示されます。

第 20 章 イベントのストア・アンド・フォワード

ストア・アンド・フォワード機能を使用して、専用のイベント・コレクター・アプライアンスからデプロイメント環境内のイベント・プロセッサー・コンポーネントにイベントを転送するためのスケジュールを管理します。

ストア・アンド・フォワード機能は、Event Collector 1501 とEvent Collector 1590 でサポートされています。これらのアプライアンスについて詳しくは、「*QRadar* ハードウェア・ガイド」を参照してください。

専用イベント・コレクターは、イベントのプロセッサーは実行しません。また、オンボードのイベント・プロセッサーも組み込まれていません。デフォルトでは、専用のイベント・コレクターが、接続先のイベント・プロセッサーに継続的にイベントを転送します。ストア・アンド・フォワード機能を使用して、イベント・コレクターからイベントを転送する時刻範囲をスケジュールすることができます。イベントが転送されない時間帯は、ローカルのアプライアンスにイベントが保管されます。IBM Security QRadar コンソールのユーザー・インターフェースでイベントにアクセスすることはできません。

業務時間内にイベントを保管するには、スケジューリング機能を使用します。転送プロセッサーがネットワーク帯域幅に影響しない時間帯に、イベントをイベント・プロセッサーに転送してください。例えば、業務時間外にイベントをイベント・プロセッサーに転送するようにイベント・コレクターを構成することができます。

関連概念:

5 ページの『IBM Security QRadar 製品の機能』
IBM Security QRadar 製品資料では、オフェンス、フロー、アセット、ヒストリカル相関などの機能について説明していますが、すべての QRadar 製品でこれらの機能を利用できるわけではありません。使用する製品によっては、説明されている一部の機能をデプロイメントで使用できない場合があります。各製品の機能を確認して、必要な情報を入手してください。

ストア・アンド・フォワードのスケジュール・リストの表示

「ストア・アンド・フォワード」ウィンドウを使用して、スケジュールのリストを表示します。スケジュールには、スケジュールの状況、パフォーマンス、および進行状況の評価に役立つ統計が含まれています。

始める前に

スケジュールを作成する必要があります。デフォルトでは、「ストア・アンド・フォワード」ウィンドウに最初にアクセスした際、スケジュールはリスト表示されません。

このタスクについて

ツールバーのオプションと「表示」リスト・ボックスのオプションを使用して、スケジュール・リストのビューを変更することができます。リストのビューを変更す

ることにより、さまざまな観点から、統計に焦点を当てます。例えば、特定のイベント・コレクターの統計を表示する場合は、「表示」リストから「イベント・コレクター **(Event Collectors)**」を選択します。これにより、リストが「イベント・コレクター **(Event Collector)**」列ごとにグループ化されるため、調査したいイベント・コレクターを簡単に探すことができます。

デフォルトでは、「ストア・アンド・フォワード」リストは、スケジュール (「表示」 > 「スケジュール」) 別に編成されたリストを表示するよう構成されています。

手順

1. 「管理」タブをクリックします。
2. ナビゲーション・メニューで、「システム構成」をクリックします。
3. 「ストア・アンド・フォワード」アイコンをクリックします。
4. 「ストア・アンド・フォワード」ウィンドウで、各スケジュールのパラメーターを確認します。

   以下の表で、スケジュールのパラメーターの一部について説明します。

表 *63.* 「ストア・アンド・フォワード」ウィンドウのパラメーター

パラメーター	説明
表示	「スケジュール」オプションは、スケジュール、イベント・プロセッサー、および関連するイベント・コレクターの間の親子関係の階層を表示します。 「イベント・コレクター」オプションは、階層の最低レベル (イベント・コレクターのリスト) を表示します。 「イベント・プロセッサー」オプションは、イベント・プロセッサーと関連するイベント・コレクターの間の親子関係の階層を表示します。

表 63. 「ストア・アンド・フォワード」ウィンドウのパラメーター (続き)

パラメーター	説明
名前	「スケジュール」オプションでは、「名前」列が以下の形式で表示されます。 • 「第 **1** レベル **(First Level)**」はスケジュールの名前を示します。 • 「第 **2** レベル **(Second Level)**」はイベント・プロセッサーの名前を示します。 • 「第 **3** レベル **(Third Level)**」はイベント・コレクターの名前を示します。 「イベント・プロセッサー」オプションでは、列が以下の形式で表示されます。 • 「第 **1** レベル **(First Level)**」はイベント・プロセッサーの名前を示します。 • 「第 **2** レベル **(Second Level)**」はイベント・コレクターの名前を示します。 **ヒント:** 階層ツリーの展開と省略を行うには、ツールバー上の名前またはオプションの横にあるプラス記号 (+) とマイナス記号 (-) を使用します。ツールバー上のオプションを使用して、階層ツリーの展開と省略を行うこともできます。
スケジュール名	「イベント・コレクター」オプションか「イベント・プロセッサー」オプションのスケジュールの名前を表示します。 1 つのイベント・プロセッサーが複数のスケジュールに関連付けられている場合、「スケジュール名」には「**複数** (*n*)」と表示されます。ここで、*n* は、スケジュールの数です。 **ヒント:** 関連付けられているスケジュールを表示するには、プラス記号 (+) をクリックします。

表 63. 「ストア・アンド・フォワード」ウィンドウのパラメーター (続き)

パラメーター	説明
最後の状況	ストア・アンド・フォワード・プロセスの状況を表示します。 • 「転送中」は、イベント転送が進行中であることを示します。 • 「転送完了」は、イベント転送が正常終了し、イベントがイベント・コレクター上でローカルに保管されていることを示します。転送を再開できることがスケジュールで指定されている場合、保管されたイベントが転送されます。 • 「警告」は、ストレージに残っているイベントのパーセンテージが、ストア・アンド・フォワード・スケジュールの残りの時間のパーセンテージを超過している、ということを示します。 • 「エラー」は、保管されているイベントがすべて転送されるより前にイベント転送が停止したことを示します。 • 「非アクティブ」は、スケジュールに割り当てられているイベント・コレクターがないか、割り当てられているイベント・コレクターがイベントをまったく受信していない、ということを示します。 **ヒント:** 「最後の状況」列にマウス・ポインターを移動すると、状況のサマリーを表示できます。
転送されたイベント	現行セッションで転送されたイベントの数を表示します (単位は K、M、G)。 **ヒント:** 「転送されたイベント」列の値にマウス・ポインターを移動すると、イベントの数を表示することができます。
残りのイベント	現行セッションで転送する残りのイベントの数を表示します (単位は K、M、G)。 **ヒント:** 「残りのイベント」列の値にマウス・ポインターを移動すると、イベントの数を表示することができます。
平均イベント・レート	イベントがイベント・コレクターからイベント・プロセッサーに転送される平均レートを表示します。 **ヒント:** 「平均イベント・レート」列の値にマウス・ポインターを移動すると、1 秒当たりのイベント数 (EPS) の平均を表示することができます。

表 63. 「ストア・アンド・フォワード」ウィンドウのパラメーター (続き)

パラメーター	説明
現在のイベント・レート	イベントがイベント・コレクターからイベント・プロセッサーに転送されているレートを表示します。 **ヒント:** 「現在のイベント・レート」列の値にマウス・ポインターを移動すると、1 秒当たりのイベント数 (EPS) の現在の値を表示することができます。
転送速度制限	転送速度制限は、構成することができます。 転送速度制限は、1 秒当たりのキロバイト数 (KB)、1 秒当たりのメガバイト数 (MB)、または 1 秒当たりのギガバイト数 (GB) で表示するように構成できます。

ストア・アンド・フォワード・スケジュールの作成

ストア・アンド・フォワード・スケジュール・ウィザードを使用して、イベント・コレクターがイベント・プロセッサーへのデータ転送の開始と停止を行うタイミングを制御するスケジュールを作成します。

複数のスケジュールを作成して管理することにより、地理的に分散したデプロイメント環境内の複数の IBM Security QRadar イベント・コレクターからのイベントの転送を制御することができます。

始める前に

専用イベント・コレクターがデプロイメント環境に追加されていて、イベント・プロセッサーに接続されているようにしてください。

手順

1. 「管理」タブをクリックします。
2. ナビゲーション・メニューで、「システム構成」をクリックします。
3. 「ストア・アンド・フォワード」アイコンをクリックします。
4. 「アクション」 > 「作成」をクリックします。
   a. 「次へ」をクリックして、「コレクターの選択 (Select Collectors)」ページに移動します。
   b. 「コレクターの選択 (Select Collectors)」ページで、パラメーターを構成します。

      構成対象のイベント・コレクターがリストされていない場合、そのイベント・コレクターが QRadar デプロイメント環境に追加されていることを確認してください。
   c. 「スケジュール・オプション (Schedule Options)」ページで、パラメーターを構成します。

転送速度の構成では、最小転送速度は 0、最大転送速度は 9,999,999 です。0 を指定すると、転送速度が無制限になります。

d. 構成を終了します。

スケジュールが「ストア・アンド・フォワード」ウィンドウで確認できるようになります。新しいスケジュールの作成後、統計が「ストア・アンド・フォワード (Store and Forward)」ウィンドウに表示されるまでに、最大で 10 分かかる場合があります。

関連タスク:

77 ページの『管理対象ホストの構成』

管理対象ホストを構成して、デプロイメント内で管理対象ホストが遂行するロールを指定します。例えば、コレクター、プロセッサー、またはデータ・ノードとして管理対象ホストを構成できます。暗号化設定の変更と、ネットワーク・アドレス変換 (NAT) グループへのホストの割り当ても実行できます。

ストア・アンド・フォワード・スケジュールの編集

ストア・アンド・フォワード・スケジュールを編集することにより、IBM Security QRadar イベント・コレクターの追加と削除、スケジュール・パラメーターの変更を行うことができます。ストア・アンド・フォワード・スケジュールを編集すると、「ストア・アンド・フォワード **(Store and Forward)**」リストに表示されている統計がリセットされます。

手順

1. 「管理」タブをクリックします。
2. ナビゲーション・メニューで、「システム構成」をクリックします。
3. 「ストア・アンド・フォワード」アイコンをクリックします。
4. 編集するスケジュールを選択します。
5. 「アクション」 > 「編集」をクリックします。

   編集したいスケジュールをダブルクリックすることもできます。
6. 「次へ」をクリックして、「コレクターの選択 (Select Collectors)」ページに移動します。
7. 「コレクターの選択 (Select Collectors)」ページで、パラメーターを編集します。
8. 「次へ」をクリックして、「スケジュール・オプション (Schedule Options)」ページに移動します。
9. 「スケジュール・オプション (Schedule Options)」ページで、スケジューリング・パラメーターを編集します。
10. 「次へ」をクリックして、「サマリー (Summary)」ページに移動します。
11. 「サマリー (Summary)」ページで、このスケジュール用に編集したオプションを確認します。

    スケジュールの編集後、統計が「ストア・アンド・フォワード (Store and Forward)」ウィンドウで更新されるまでに、最大で 10 分かかる場合があります。

ストア・アンド・フォワード・スケジュールの削除

「ストア・アンド・フォワード」スケジュールを削除することができます。

手順

1. ナビゲーション・メニューで、「システム構成」をクリックします。
2. 「ストア・アンド・フォワード」アイコンをクリックします。
3. 削除したいスケジュールを選択します。
4. 「アクション」 > 「削除」をクリックします。

スケジュールが削除されると、関連する IBM Security QRadar イベント・コレクターにより、割り当てられているイベント・プロセッサーへのイベントの継続的な転送が再開されます。

第 21 章 セキュリティー・コンテンツ

IBM Security QRadar のコンテンツ・マネジメント・ツールを使用して、セキュリティー・コンテンツ (ルール、レポート、ダッシュボードおよびアプリケーションなど) を QRadar にインポートします。セキュリティー・コンテンツを他の QRadar システムから導入するか自身で開発して、既存の QRadar 機能を拡張することができます。

関連概念:

5 ページの『IBM Security QRadar 製品の機能』
IBM Security QRadar 製品資料では、オフェンス、フロー、アセット、ヒストリカル相関などの機能について説明していますが、すべての QRadar 製品でこれらの機能を利用できるわけではありません。使用する製品によっては、説明されている一部の機能をデプロイメントで使用できない場合があります。各製品の機能を確認して、必要な情報を入手してください。

セキュリティー・コンテンツのタイプ

IBM Security QRadar のコンテンツは、コンテンツ・パックと拡張の 2 つのタイプにまとめられます。

コンテンツ・パック

セキュリティー・コンテンツ・パック には、特定のタイプのセキュリティー・コンテンツに対する機能拡張が含まれています。多くの場合、サード・パーティー統合やオペレーティング・システム用のコンテンツが含まれています。例えば、サード・パーティー統合用のセキュリティー・コンテンツ・パックには、イベント・ペイロードの情報からログ・ソースを検索してレポートに使用できるようにする新しいカスタム・イベント・プロパティーが含まれている場合があります。

セキュリティー・コンテンツ・パックは IBM Fix Central (http://www.ibm.com/support/fixcentral) から入手できます。コンテンツ・パックは自動更新の一環として入手することはできません。

拡張

IBM や他のベンダーは、QRadar の機能を拡張するセキュリティー拡張 を作成します。拡張には、アプリケーションやコンテンツ項目 (カスタム・ルール、レポート・テンプレート、保存済み検索など) が含まれている場合も、既存のコンテンツ項目に対する更新が含まれている場合もあります。例えば、オフェンスの情報を視覚化するためのタブを QRadar に追加するアプリケーションを含む拡張があります。

IBM Security App Exchange では、拡張はアプリケーションとして認識されています。QRadar アプリケーションは、IBM Security App Exchange からダウンロードし、「拡張の管理」ツールを使用してインストールできます。アプリケーションは、自動更新の一環として入手することはできません。

セキュリティー・コンテンツのソース

QRadar のコンテンツは以下のソースから使用できます。

IBM Security App Exchange
IBM Security App Exchange (https://apps.xforce.ibmcloud.com) はアプリケーション・ストア兼ポータルであり、QRadar 拡張機能を参照してダウンロードすることができます。この新しい方法でコード、視覚化、レポート、ルール、およびアプリケーションを共有することができます。

IBM Fix Central
IBM Fix Central (www.ibm.com/support/fixcentral) では、システム・ソフトウェア、ハードウェア、およびオペレーティング・システムに対する修正および更新を提供しています。IBM Fix Central からセキュリティー・コンテンツ・パックおよび拡張をダウンロードすることができます。

QRadar デプロイメント
コンテンツを再利用するときは、QRadar デプロイメントからカスタム・コンテンツを拡張としてエクスポートし、別のシステムにインポートします。例えば、開発環境から実稼働環境にコンテンツをエクスポートできます。コンテンツ管理スクリプトを使用すると、すべてのコンテンツをエクスポートしたり、一部のカスタム・コンテンツのみをエクスポートしたりすることができます。

コンテンツのインポートおよびエクスポートの方式

以下のツールを使用して、IBM Security QRadar デプロイメントのコンテンツをインポートおよびエクスポートできます。

「拡張の管理」ツール

「拡張の管理」ツールを使用して、QRadar デプロイメントに拡張を追加します。「拡張の管理」ツールを使用してコンテンツをインポートする場合は、コンテンツをインストールする前に表示することができます。そのコンテンツ項目がシステムに存在する場合、コンテンツ項目を置換するか、更新をスキップするかを指定できます。

コンテンツをエクスポートするときには「拡張の管理」ツールは使用できません。

コンテンツ管理スクリプト

コンテンツ管理スクリプトを使用して、カスタム・コンテンツを QRadar デプロイメントから外部のポータブル形式でエクスポートします。その後このスクリプトを使用して、カスタム・コンテンツを別の QRadar デプロイメントにインポートできます。このスクリプトは、QRadar デプロイメント間でのコンテンツ移動を自動化する場合に役立ちます。

`contentManagement.pl` スクリプトが `/opt/qradar/bin` ディレクトリーにあります。

QRadar ソース・デプロイメントからコンテンツをエクスポートするには、コンテンツ管理スクリプトを使用する必要があります。コンテンツ管理スクリプトまたは

「拡張の管理」ツールのいずれかを使用して、コンテンツをターゲット・デプロイメントにインポートできます。

すべてのカスタム・コンテンツのエクスポート

contentManagement.pl スクリプトを使用して、IBM Security QRadar デプロイメント内のすべてのカスタム・コンテンツをエクスポートします。

手順

1. SSH を使用して、root ユーザーとして QRadar にログインします。
2. /opt/qradar/bin ディレクトリーに移動し、以下のコマンドを入力してすべてのカスタム・コンテンツをエクスポートします。

   ```
   ./contentManagement.pl -a export -c all
   ```

   例:

   - エクスポートに集計データを含めるには、以下のコマンドを入力します。

     ```
     ./contentManagement.pl --action export --content-type all -g
     ```

   - エクスポートするファイルのディレクトリーを指定し、圧縮形式を変更するには、以下のコマンドを入力します。

     ```
     ./contentManagement.pl -a export -c all -o [filepath] -t [compression_type]
     ```

タスクの結果

コンテンツが圧縮ファイル (例えば all-ContentExport-20151022101803.zip) にエクスポートされます。ファイル名は分かりやすい名前に手動で変更できます。エクスポートされたファイルには、予想よりも多くのコンテンツが含まれている場合があります。これは、指定されたコンテンツ項目とともにすべての依存関係がエクスポートされるためです。例えば、レポートをエクスポートすると、そのレポートで使用される保存済み検索もエクスポートされます。

特定のタイプのすべてのカスタム・コンテンツのエクスポート

特定のタイプのすべてのカスタム・コンテンツを 1 回のアクションでエクスポートできます。

このタスクについて

コンテンツ・マネジメント・スクリプトでは、テキスト ID または数値 ID を使用して、エクスポートするコンテンツのタイプを指定します。

表 *64.* カスタム・コンテンツのエクスポートのためのコンテンツ・タイプ *ID*

カスタム・コンテンツのタイプ	テキスト **ID**	数値 **ID**
ダッシュボード	**dashboard**	4
レポート	**report**	10
保存済み検索	**search**	1
FGroup [1]	**fgroup**	12
FGroup タイプ	**fgrouptype**	13
カスタム・ルール	**customrule**	3

表 64. カスタム・コンテンツのエクスポートのためのコンテンツ・タイプ ID (続き)

カスタム・コンテンツのタイプ	テキスト ID	数値 ID
カスタム・プロパティー	**customproperty**	6
ログ・ソース	**sensordevice**	17
ログ・ソース・タイプ	**sensordevicetype**	24
ログ・ソース・カテゴリー	**sensordevicecategory**	18
ログ・ソース拡張	**deviceextension**	16
リファレンス・データ収集	**referencedata**	28
カスタム QID マップ項目	**qidmap**	27
ヒストリカル相関プロファイル	**historicalsearch**	25
カスタム関数	**custom_function**	77
カスタム・アクション	**custom_action**	78
アプリケーション	**installed_application**	100
DSM イベント・マッピング	**dsmevent**	41
[1]FGroup は、コンテンツ・グループ (ログ・ソース・グループ、レポート作成グループ、検索グループなど) を表します。		

手順

1. SSH を使用して、root ユーザーとして IBM Security QRadar にログインします。
2. /opt/qradar/bin ディレクトリーに移動し、以下のコマンドを入力して指定したタイプのコンテンツをすべてエクスポートします。

   ```
   ./contentManagement.pl -a export --content-type [content_type] --id all
   ```

   パラメーター:

表 65. 特定タイプのカスタム・コンテンツをエクスポートするための *contentManagement.pl* スクリプト・パラメーター

パラメーター	説明
-c *[content_type]* または **--content-type** *[content_type]*	コンテンツのタイプを指定します。 対応するテキスト ID または数値 ID を入力して、コンテンツ・タイプを指定できます。
-e または **--include-reference-data-elements**	リファレンス・データのキーとエレメントをエクスポートに含めるには、このフラグを設定します。 リファレンス・データ・キーおよびリファレンス・データ・エレメントは referencedata コンテンツ・タイプに適用できます。このパラメーターは、リファレンス・データ、またはリファレンス・データに基づくコンテンツ項目をエクスポートする場合にのみ適用できます。

表 65. 特定タイプのカスタム・コンテンツをエクスポートするための *contentManagement.pl* スクリプト・パラメーター (続き)

パラメーター	説明
-g または **--global-view**	エクスポートに集計データを含めます。
-i *[content_identifier]* または **--id** *[content_identifier]*	カスタム・コンテンツの特定のインスタンス (単一のレポートや単一のリファレンス・セットなど) の ID を指定します。 指定したタイプのコンテンツをすべてエクスポートする場合は、*all* を指定できます。
-o *[filepath]* または **--output-directory** *[filepath]*	エクスポート・ファイルの書き込み先のディレクトリーの絶対パスを指定します。 出力ディレクトリーが指定されていない場合、コンテンツは現行ディレクトリーにエクスポートされます。指定された出力ディレクトリーが存在しない場合は、そのディレクトリーが作成されます。
-t *[compression_type]* または **--compression-type** *[compression_type]*	エクスポート・ファイルの圧縮タイプを指定します。 有効なオプションは `ZIP` および `TARGZ` です (大/小文字の区別あり)。圧縮タイプを指定しない場合、デフォルトの圧縮タイプ `ZIP` が使用されます。

例:

- すべてのカスタム検索をエクスポートするには、以下のコマンドを入力します。

  ```
  ./contentManagement.pl --action export --content-type search --id all
  ```

- すべてのレポートをエクスポートし、集計データを含めるには、以下のコマンドを入力します。

  ```
  ./contentManagement.pl -a export -c 10 --id all --global-view
  ```

タスクの結果

コンテンツが圧縮ファイル (例えば `reports-ContentExport-20151022101803.zip`) にエクスポートされます。ファイル名は分かりやすい名前に手動で変更できます。エクスポートされたファイルには、予想よりも多くのコンテンツが含まれている場合があります。これは、指定されたコンテンツ項目とともにすべての依存関係がエクスポートされるためです。例えば、レポートをエクスポートすると、そのレポートで使用される保存済み検索もエクスポートされます。

エクスポートする特定のコンテンツ項目の検索

コンテンツ管理スクリプトを使用して、IBM Security QRadar デプロイメント内の特定のコンテンツを検索します。コンテンツを検出したら、固有 ID を使用してコンテンツ項目をエクスポートできます。

このタスクについて

以下の表に、特定のタイプのコンテンツを検索する際に使用する ID をリストします。

表 *66.* カスタム・コンテンツの検索のためのコンテンツ・タイプ *ID*

カスタム・コンテンツのタイプ	テキスト **ID**	数値 **ID**
ダッシュボード	**dashboard**	4
レポート	**report**	10
保存済み検索	**search**	1
FGroup [1]	**fgroup**	12
FGroup タイプ	**fgrouptype**	13
カスタム・ルール	**customrule**	3
カスタム・プロパティー	**customproperty**	6
ログ・ソース	**sensordevice**	17
ログ・ソース・タイプ	**sensordevicetype**	24
ログ・ソース・カテゴリー	**sensordevicecategory**	18
ログ・ソース拡張	**deviceextension**	16
リファレンス・データ収集	**referencedata**	28
カスタム QID マップ項目	**qidmap**	27
ヒストリカル相関プロファイル	**historicalsearch**	25
カスタム関数	**custom_function**	77
カスタム・アクション	**custom_action**	78
アプリケーション	**installed_application**	100
[1]FGroup は、コンテンツ・グループ (ログ・ソース・グループ、レポート作成グループ、検索グループなど) を表します。		

手順

1. SSH を使用して、root ユーザーとして QRadar にログインします。
2. /opt/qradar/bin ディレクトリーに移動し、以下のコマンドを入力して正規表現に一致するカスタム・コンテンツを検索します。

   ```
   ./contentManagement.pl -a search -c [content_type] -r [regex]
   ```

   パラメーター:

表 67. コンテンツ項目を検索するための *contentManagement.pl* スクリプト・パラメーター

パラメーター	説明
-c *[content_type]* または **--content-type** *[content_type]*	検索するコンテンツのタイプを指定します。 検索するコンテンツのタイプを指定する必要があります。search アクションでは -c package および -c all は使用できません。
-r *[regex]* または **--regex** *[regex]*	検索するコンテンツを指定します。 式に一致するすべてのコンテンツが表示されます。

例:

- 記述内容に Overview が含まれるすべてのレポートを検索するには、以下のコマンドを入力します。

  ```
  /opt/qradar/bin/contentManagement.pl --action search
  --content-type report --regex "Overview"
  ```

- すべてのログ・ソースをリストするには、次のコマンドを入力します。

  ```
  /opt/qradar/bin/contentManagement.pl -a search -c 17 -r "¥w"
  ```

検索結果には、検出されたコンテンツ項目の詳細 (固有 ID を含む) がリストされます。

```
[INFO] Search results:
[INFO] - [ID] - [Name] - [Description]
[INFO] - [67] - [Asset Profiler-2 :: hostname] - [Asset Profiler]
[INFO] - [62] - [SIM Generic Log DSM-7 :: hostname] - [SIM Generic Log DSM]
[INFO] - [63] - [Custom Rule Engine-8 :: hostname] - [Custom Rule Engine]
[INFO] - [71] - [Pix @ apophis] - [Pix device]
[INFO] - [70] - [Snort @ wolverine] - [Snort device]
[INFO] - [64] - [SIM Audit-2 :: hostname] - [SIM Audit]
[INFO] - [69] - [Health Metrics-2 :: hostname] - [Health Metrics]
```

次のタスク

QRadar から特定のコンテンツ項目をエクスポートするには、固有 ID を使用します。詳しくは、 325 ページの『異なるタイプのカスタム・コンテンツ項目のエクスポート』および『単一のカスタム・コンテンツ項目のエクスポート』を参照してください。

単一のカスタム・コンテンツ項目のエクスポート

IBM Security QRadar から、カスタム・ルール、保存済み検索などの単一のカスタム・コンテンツ項目をエクスポートします。

始める前に

エクスポートするカスタム・コンテンツ項目の固有 ID が分かっている必要があります。コンテンツ項目の固有 ID の検出について詳しくは、 322 ページの『エクスポートする特定のコンテンツ項目の検索』を参照してください。

手順

1. SSH を使用して、root ユーザーとして QRadar にログインします。
2. /opt/qradar/bin ディレクトリーに移動し、以下のコマンドを入力してコンテンツをエクスポートします。

   ```
   ./contentManagement.pl -a export -c [content_type] -i [content_identifier]
   ```

   パラメーター:

表 68. 単一のコンテンツ項目をエクスポートするための *contentManagement.pl* スクリプト・パラメーター

パラメーター	説明
-c *[content_type]* または **--content-type** *[content_type]*	エクスポートするコンテンツのタイプを指定します。 特定のコンテンツ・タイプに対応するテキスト ID または数値 ID を入力します。
-e または **--include-reference-data-elements**	リファレンス・データのキーとエレメントをエクスポートに含めるには、このフラグを設定します。 リファレンス・データ・キーおよびリファレンス・データ・エレメントは referencedata コンテンツ・タイプに適用できます。このパラメーターは、リファレンス・データ、またはリファレンス・データに基づくコンテンツ項目をエクスポートする場合にのみ適用できます。
-g または **--global-view**	エクスポートに集計データを含めます。
-i *[content_identifier]* または **--id** *[content_identifier]*	カスタム・コンテンツの特定のインスタンス (単一のレポートや単一のリファレンス・セットなど) の ID を指定します。
-o *[filepath]* または **--output-directory** *[filepath]*	エクスポート・ファイルの書き込み先のディレクトリーの絶対パスを指定します。 出力ディレクトリーが指定されていない場合、コンテンツは現行ディレクトリーにエクスポートされます。指定された出力ディレクトリーが存在しない場合は、そのディレクトリーが作成されます。
-t *[compression_type]* または **--compression-type** *[compression_type]*	export アクションで使用します。 エクスポート・ファイルの圧縮タイプを指定します。有効なオプションは ZIP および TARGZ です (大/小文字の区別あり)。圧縮タイプを指定しない場合、デフォルトの圧縮タイプ ZIP が使用されます。

例:

- ID が 7 のダッシュボードを現行ディレクトリーにエクスポートするには、以下のコマンドを入力します。

  ```
  ./contentManagement.pl -a export -c dashboard -i 7
  ```

- 集計データを含む ID が 70 のログ・ソースを /store/cmt/exports ディレクトリーにエクスポートするには、次のコマンドを入力します。

  ```
  ./contentManagement.pl -a export -c sensordevice -i 70 -o /store/cmt/exports -g
  ```

タスクの結果

コンテンツは .zip 圧縮ファイルにエクスポートされます。エクスポートされたファイルには、予想よりも多くのコンテンツが含まれている場合があります。これは、指定されたコンテンツ項目とともにすべての依存関係がエクスポートされるためです。例えば、レポートをエクスポートすると、そのレポートで使用される保存済み検索もエクスポートされます。ファイル名は分かりやすい名前に手動で変更できます。

異なるタイプのカスタム・コンテンツ項目のエクスポート

コンテンツ管理スクリプトを使用して、IBM Security QRadar から複数のカスタム・コンテンツ項目 (カスタム・ルール、ダッシュボード、レポートなど) をエクスポートします。

始める前に

エクスポートする各カスタム・コンテンツ項目の固有 ID が分かっている必要があります。コンテンツ項目の固有 ID の検出について詳しくは、 322 ページの『エクスポートする特定のコンテンツ項目の検索』を参照してください。

手順

1. SSH を使用して、root ユーザーとして QRadar にログインします。
2. エクスポートするコンテンツをリストするテキスト・ファイルを作成します。

   各行に、カスタム・コンテンツ・タイプを入力し、その後にそのタイプの固有 ID のコンマ区切りリストを入力します。

   例: ID が 5 と ID が 7 の 2 つのダッシュボード、すべてのカスタム・ルール、および 1 つのグループをエクスポートするには、次の項目を含むテキスト・ファイルを作成します。

   ```
   dashboard, 5,7
   customrule, all
   fgroup, 77
   ```

3. /opt/qradar/bin に移動し、コンテンツをエクスポートするコマンドを入力します。

   ```
   ./contentManagement.pl -a export -c package -f [source_file]
   ```

   パラメーター:

表 69. 各タイプのコンテンツ項目をエクスポートするための *contentManagement.pl* スクリプト・パラメーター

パラメーター	説明
-c *[content_type]* または **--content-type** *[content_type]*	コンテンツのタイプを指定します。 -c package を指定するか、特定のコンテンツ・タイプに対応するテキスト ID または数値 ID を入力できます。-c package を使用する場合、--file パラメーターまたは --name パラメーターを指定する必要があります。
-e または **--include-reference-data-elements**	リファレンス・データのキーとエレメントをエクスポートに含めるには、このフラグを設定します。 リファレンス・データ・キーおよびリファレンス・データ・エレメントは referencedata コンテンツ・タイプに適用できます。このパラメーターは、リファレンス・データ、またはリファレンス・データに基づくコンテンツ項目をエクスポートする場合にのみ適用できます。
-f *[source_file]* または **--file** *[source_file]*	エクスポートするカスタム・コンテンツ項目のリストを含むテキスト・ファイルのパスとファイル名を指定します。 --file パラメーターを初めて使用すると、パッケージ・テンプレート・ファイルが /store/cmt/packages ディレクトリーに書き込まれるため、それを再使用できます。 ファイル名とパスは、大/小文字の区別があります。
-g または **--global-view**	エクスポートに集計データを含めます。
-n *[name]* または **--name** *[name]*	エクスポートするカスタム・コンテンツのリストを含むパッケージ・テンプレート・ファイルの名前を指定します。 パッケージ・テンプレート・ファイルは、--file パラメーターを初めて使用したときに作成されます。--name パラメーターを使用する場合、デフォルトでは、テキスト・ファイルが /store/cmt/packages ディレクトリーにあると見なされます。 --content-type package を使用する場合は、--file または --name パラメーターを指定する必要があります。

表 69. 各タイプのコンテンツ項目をエクスポートするための *contentManagement.pl* スクリプト・パラメーター (続き)

パラメーター	説明
-o *[filepath]* または **--output-directory** *[filepath]*	エクスポート・ファイルの書き込み先のディレクトリーの絶対パスを指定します。 出力ディレクトリーが指定されていない場合、コンテンツは現行ディレクトリーにエクスポートされます。指定された出力ディレクトリーが存在しない場合は、そのディレクトリーが作成されます。
-t *[compression_type]* または **--compression-type** *[compression_type]*	エクスポート・ファイルの圧縮タイプを指定します。 有効な圧縮タイプは ZIP および TARGZ です (大/小文字の区別あり)。圧縮タイプを指定しない場合、デフォルトの圧縮タイプ ZIP が使用されます。

例:

- qradar ディレクトリー内の exportlist.txt ファイルのすべての項目をエクスポートし、エクスポートされたファイルを現行ディレクトリーに保存するには、以下のコマンドを入力します。

  ```
  ./contentManagement.pl -a export -c package -f /qradar/exportlist.txt
  ```

- qradar ディレクトリー内の exportlist.txt ファイルのすべての項目 (集計データを含む) をエクスポートし、出力を /store/cmt/exports ディレクトリーに保存するには、以下のコマンドを入力します。

  ```
  ./contentManagement.pl -a export -c package
  --file /qradar/exportlist.txt -o /store/cmt/exports -g
  ```

--file パラメーターを使用すると、パッケージ・テンプレート・ファイルが /store/cmt/packages に自動的に生成されます。このパッケージ・テンプレート・ファイルを使用するには、**--name** パラメーターの値として、このファイル名を指定します。

タスクの結果

コンテンツは .zip 圧縮ファイルにエクスポートされます。エクスポートされたファイルには、予想よりも多くのコンテンツが含まれている場合があります。これは、指定されたコンテンツ項目とともにすべての依存関係がエクスポートされるためです。例えば、レポートをエクスポートすると、そのレポートで使用される保存済み検索もエクスポートされます。ファイル名は分かりやすい名前に手動で変更できます。

「拡張の管理」を使用した拡張のインストール

「拡張の管理」ツールを使用すると、IBM Security QRadar にセキュリティー拡張を追加できます。「拡張の管理」ツールでは、拡張のインストール前に、拡張のコンテンツ項目を表示すること、およびコンテンツの更新を処理する方法を指定することができます。

始める前に

QRadar に拡張をインストールする前に、それらの拡張をローカル・コンピューターに配置する必要があります。

QRadar の拡張は、IBM Security App Exchange (https://apps.xforce.ibmcloud.com/) から、および IBM Fix Central (www.ibm.com/support/fixcentral/) からダウンロードできます。

このタスクについて

拡張は、QRadar 機能のバンドルです。拡張には、ルール、レポート、検索、リファレンス・セット、ダッシュボードなどのコンテンツを含めることができます。また、QRadar 機能を強化するアプリケーションを含めることもできます。

手順

1. 「管理」タブで、「拡張の管理」をクリックします。
2. QRadar コンソールに新しい拡張をアップロードするには、以下の手順に従います。
   a. 「追加」をクリックします。
   b. 「参照」をクリックし、ナビゲートして拡張を見つけます。
   c. オプション: 「即時にインストール」をクリックすると、コンテンツを表示せずに拡張をインストールできます。
   d. 「追加」をクリックします。
3. 拡張のコンテンツを表示するには、拡張のリストからその拡張を選択し、「詳細」をクリックします。
4. 拡張をインストールするには、以下の手順に従います。
   a. リストから拡張を選択し、「インストール」をクリックします。
   b. 拡張にデジタル署名が含まれていない場合、または署名がある一方で、その署名が IBM Security Certificate Authority (CA) に関連付けられていない場合、その拡張をインストールするか確認する必要があります。インストールを続行する場合は、「インストール」をクリックします。
   c. インストールにより行われるシステムの変更を確認します。
   d. 「上書き」または「既存データを保持」を選択して、既存のコンテンツ項目の処理方法を指定します。
   e. 「インストール」をクリックします。
   f. インストール・サマリーを確認し、「**OK**」をクリックします。

コンテンツ管理スクリプトを使用したコンテンツのインポート

別の IBM Security QRadar システムからエクスポートしたカスタム・コンテンツをインポートできます。

始める前に

別の QRadar システムからコンテンツをインポートする場合、最初にコンテンツをエクスポートし、次にそのコンテンツをターゲット・システムにコピーする必要が

あります。コンテンツのエクスポートについて詳しくは、 331 ページの『カスタム・コンテンツのエクスポートのためのコンテンツ・タイプ ID』を参照してください。

ログ・ソースを含むコンテンツをインポートする場合、DSM とプロトコル RPM がターゲット・システムにインストールされていること、およびそれらが最新であることを確認してください。

同一システム上で同時に複数のインポートを開始しないでください。共有リソースの競合が原因でインポートは失敗します。

手順

1. SSH を使用して、root ユーザーとして QRadar にログインします。
2. エクスポート・コンテンツ・ファイルが配置されているディレクトリーに移動します。
3. 以下のコマンドを入力して、コンテンツをインポートします。

   ```
   /opt/qradar/bin/contentManagement.pl -a import -f [source_file] -u [user]
   ```

   パラメーター:

表 70. カスタム・コンテンツをインポートするための *contentManagement.pl* スクリプト・パラメーター

パラメーター	説明
-f *[source_file]* または **--file** *[source_file]*	インポートするコンテンツ項目を含むファイルを指定します。 有効なファイル・タイプは zip、targz、および xml です。 ファイル名とパスは、大/小文字の区別があります。
-u *[user]* または **--user** *[user]*	ユーザー固有のデータをインポートするときに、現行所有者を置き換えるユーザーを指定します。このユーザーは、コンテンツのインポート前にターゲット・システムに存在している必要があります。

   例:

   - fgroup-ContentExport-20120418163707.tar.gz ファイルから現行ディレクトリーにコンテンツをインポートするには、以下のコマンドを入力します。

     ```
     /opt/qradar/bin/contentManagement.pl --action import
     -f fgroup-ContentExport-20120418163707.tar.gz
     ```

   - fgroup-ContentExport-20120418163707.tar.gz ファイルから現行ディレクトリーにコンテンツをインポートし、インポートのすべての機密データの所有者を admin ユーザーにするには、以下のコマンドを入力します。

     ```
     /opt/qradar/bin/contentManagement.pl --action import
     --file fgroup-ContentExport-20120418163707.tar.gz --user admin
     ```

   リファレンス・データのエクスポート時にそのリファレンス・データが収集されている場合、インポート・スクリプトにより「**外部キー制約違反** (Foreign key

constraint violation)」というメッセージが表示されます。この問題を防止するには、リファレンス・データが収集されていないときにエクスポート・プロセスを実行します。

コンテンツ管理スクリプトを使用したコンテンツの更新

既存の IBM Security QRadar コンテンツを更新するか、またはシステムに新規コンテンツを追加するには、update アクションを使用します。

始める前に

他の QRadar システムからエクスポートしたコンテンツを使用してコンテンツを更新する場合、エクスポートしたファイルがターゲット・システムにあることを確認します。コンテンツのエクスポートについて詳しくは、 331 ページの『カスタム・コンテンツのエクスポートのためのコンテンツ・タイプ ID』を参照してください。

ログ・ソースを含むコンテンツをインポートする場合、DSM とプロトコル RPM がターゲット・システムにインストールされていること、およびそれらが最新であることを確認してください。

同一システム上で同時に複数のインポートを開始しないでください。共有リソースの競合が原因でインポートは失敗します。

手順

1. SSH を使用して、root ユーザーとして QRadar にログインします。
2. コンテンツを更新するために、以下のコマンドを入力します。

   ```
   /opt/qradar/bin/contentManagement.pl -a update -f [source_file]
   ```

   パラメーター:

表 71. カスタム・コンテンツを更新するための *contentManagement.pl* スクリプト・パラメーター

パラメーター	説明
-f *[source_file]* または **--file** *[source_file]*	更新するコンテンツ項目を含むファイルを指定します。 有効なファイル・タイプは zip、targz、および xml です。 ファイル名とパスは、大/小文字の区別があります。
-u *[user]* または **--user** *[user]*	ユーザー固有のデータをインポートするときに、現行所有者を置き換えるユーザーを指定します。 このユーザーは、コンテンツのインポート前にターゲット・システムに存在している必要があります。

   例:

   - fgroup-ContentExport-20120418163707.zip ファイル内のコンテンツに基づいて更新するには、以下のコマンドを入力します。

```
/opt/qradar/bin/contentManagement.pl --action update
-f fgroup-ContentExport-20120418163707.zip
```

IBM Fix Central からのコンテンツ・パックの手動インストール

コマンド・ラインを使用してコンテンツ・パックをインストールします。

手順

1. コンテンツ・パック (RPM ファイル) を IBM Fix Central (www.ibm.com/support/fixcentral) からダウンロードします。
2. RPM ファイルを QRadar コンソールにコピーします。
3. SSH を使用して、root ユーザーとして QRadar にログインします。
4. ダウンロードしたファイルが入っているディレクトリーから次のコマンドを入力します。

   ```
   rpm -Uvh filename
   ```
5. QRadar に管理者としてログインします。
6. 「管理」タブで、「拡張」 > 「**Web** サーバーの再始動」を選択して Tomcat を再始動します。

カスタム・コンテンツのエクスポートのためのコンテンツ・タイプ ID

特定のタイプのカスタム・コンテンツを IBM Security QRadar からエクスポートするには、コンテンツ・タイプを指定する必要があります。コンテンツ・タイプにはテキスト ID または数値 ID のいずれかを使用する必要があります。

QRadar アプライアンスからコンテンツをエクスポートする際に、コンテンツ管理スクリプトにより依存関係がチェックされ、関連するコンテンツがエクスポートに組み込まれます。

例えば、コンテンツ管理スクリプトにより、エクスポート対象のレポートに保存済み検索が関連付けられていることが検出されると、その保存済み検索もエクスポートされます。オフェンス、アセット、または脆弱性の保存済み検索をエクスポートすることはできません。

特定のタイプのすべてのカスタム・コンテンツをエクスポートする場合は、コンテンツ・タイプ ID を使用します。QRadar デプロイメントから特定のコンテンツ項目をエクスポートする場合は、そのコンテンツ項目の固有 ID を知っていなければなりません。詳しくは、 322 ページの『エクスポートする特定のコンテンツ項目の検索』を参照してください。

`contentManagement.pl` スクリプトに **-c** パラメーターで渡すコンテンツ・タイプ ID を以下の表に示します。

表 *72.* カスタム・コンテンツのエクスポートのためのコンテンツ・タイプ *ID*

カスタム・コンテンツのタイプ	テキスト **ID**	数値 **ID**
すべてのカスタム・コンテンツ	**all**	適用外

表 72. カスタム・コンテンツのエクスポートのためのコンテンツ・タイプ ID (続き)

カスタム・コンテンツのタイプ	テキスト ID	数値 ID
コンテンツのカスタム・リスト	**package**	適用外
ダッシュボード	**dashboard**	4
レポート	**report**	10
保存済み検索	**search**	1
FGroup [1]	**fgroup**	12
FGroup タイプ	**fgrouptype**	13
カスタム・ルール	**customrule**	3
カスタム・プロパティー	**customproperty**	6
ログ・ソース	**sensordevice**	17
ログ・ソース・タイプ	**sensordevicetype**	24
ログ・ソース・カテゴリー	**sensordevicecategory**	18
ログ・ソース拡張	**deviceextension**	16
リファレンス・データ収集	**referencedata**	28
カスタム QID マップ項目	**qidmap**	27
ヒストリカル相関プロファイル	**historicalsearch**	25
カスタム関数	**custom_function**	77
カスタム・アクション	**custom_action**	78
アプリケーション	**installed_application**	100
[1]FGroup は、コンテンツ・グループ (ログ・ソース・グループ、レポート作成グループ、検索グループなど) です。		

コンテンツ管理スクリプトのパラメーター

contentManagement.pl スクリプトを使用して、IBM Security QRadar デプロイメントからコンテンツをエクスポートし、別のデプロイメントにインポートします。

次の表で、contentManagement.pl スクリプトのパラメーター、および各パラメーターが適用されるアクションについて説明します。

/opt/qradar/bin/contentManagement.pl --action *[action_type] [script_parameters]*

表 73. *contentManagement.pl* スクリプト・パラメーター

パラメーター	説明
-a *[action_type]* または **--action** *[action_type]*	必須。アクションを指定します。 有効なアクション・タイプは、export、search、import、および update です。 import アクションは、デプロイメントに存在していないコンテンツだけを追加します。

表 73. *contentManagement.pl* スクリプト・パラメーター (続き)

パラメーター	説明
-c *[content_type]* または **--content-type** *[content_type]*	export アクションおよび search アクションで使用します。コンテンツのタイプを指定します。 export アクションで使用するときは、-c all または -c package を指定するか、特定のコンテンツ・タイプに対応するテキスト ID または数値 ID を入力できます。-c package を使用する場合、--file パラメーターまたは --name パラメーターを指定する必要があります。 search アクションで使用する場合、検索するコンテンツのタイプを指定する必要があります。search アクションでは -c package および -c all は使用できません。
-d または **--debug**	すべてのアクションで使用します。 contentManagement.pl スクリプトを実行して、詳しい情報 (お客様サポート用のログなど) を表示するときに、デバッグ・レベル・ロギングを使用します。
-e または **--include-reference-data-elements**	export アクションで使用します。 リファレンス・データのキーとエレメントをエクスポートに含めるには、このフラグを設定します。 リファレンス・データ・キーおよびリファレンス・データ・エレメントは referencedata コンテンツ・タイプに適用できます。このパラメーターは、リファレンス・データ、またはリファレンス・データに基づくコンテンツ項目をエクスポートする場合にのみ適用できます。
-f *[file_path]* または **--file** *[file_path]*	export、import、および update アクションで使用します。 export アクションで使用する場合、エクスポートするカスタム・コンテンツ項目のリストを含むテキスト・ファイルのパスとファイル名を指定します。--file パラメーターを初めて使用すると、パッケージ・テンプレート・ファイルが /store/cmt/packages ディレクトリーに書き込まれるため、それを再使用できます。 import アクションまたは update アクションで使用する場合、インポートするコンテンツ項目を含むファイルを指定します。有効なファイル・タイプは zip、targz、および xml です。 ファイル名とパスは、大/小文字の区別があります。

表 73. *contentManagement.pl* スクリプト・パラメーター (続き)

パラメーター	説明
-g または **--global-view**	export アクションで使用します。 エクスポートに集計データを含めます。
-h *[action_type]* または **--help** *[action_type]*	すべてのアクションで使用します。 action_type に固有のヘルプを表示します。action_type が指定されていない場合、一般ヘルプ・メッセージを表示します。
-i *[content_identifier]* または **--id** *[content_identifier]*	export アクションで使用します。 カスタム・コンテンツの特定のインスタンス (単一のレポートや単一のリファレンス・セットなど) の ID を指定します。指定したタイプのコンテンツをすべてエクスポートする場合は、*all* を指定できます。
-n *[name]* または **--name** *[name]*	export アクションで使用します。 エクスポートするカスタム・コンテンツのリストを含むパッケージ・テンプレート・ファイルの名前を指定します。 パッケージ・テンプレート・ファイルは、--file パラメーターを初めて使用したときに作成されます。--name パラメーターを使用する場合、テンプレート・ファイルが /store/cmt/packages ディレクトリーにあると見なされます。 --content-type package を使用する場合は、--file または --name パラメーターを指定する必要があります。
-o *[filepath]* または **--output-directory** *[filepath]*	export アクションで使用します。 エクスポート・ファイルの書き込み先のディレクトリーの絶対パスを指定します。 出力ディレクトリーが指定されていない場合、コンテンツは現行ディレクトリーにエクスポートされます。指定された出力ディレクトリーが存在しない場合は、そのディレクトリーが作成されます。
-q または **--quiet**	すべてのアクションで使用します。画面に出力が表示されません。
-r *[regex]* または **--regex** *[regex]*	search アクションで使用します。 検索する場合、--regex パラメーターを使用して、検索するコンテンツを指定する必要があります。式に一致するすべてのコンテンツが表示されます。

表 73. *contentManagement.pl* スクリプト・パラメーター (続き)

パラメーター	説明
-t *[compression_type]* または **--compression-type** *[compression_type]*	export アクションで使用します。 エクスポート・ファイルの圧縮タイプを指定します。有効な圧縮タイプは ZIP および TARGZ です (大/小文字の区別あり)。圧縮タイプを指定しない場合、デフォルトの圧縮タイプ ZIP が使用されます。
-u *[user]* または **--user** *[user]*	import アクションで使用します。 ユーザー固有のデータをインポートするときに、現行所有者を置き換えるユーザーを指定します。このユーザーは、コンテンツのインポート前にターゲット・システムに存在している必要があります。
-v または **--verbose**	すべてのアクションで使用します。 ログインする際に使用して、コンテンツ・マネジメント・ツールのデフォルト・レベルの情報を表示します。

第 22 章 SNMP トラップ構成

IBM Security QRadar は、さまざまなシステム・リソースのモニター MIB をサポートする Net-SNMP エージェントを使用します。システム・リソースをモニターし通知するために、ネットワーク管理ソリューションによって、これらの MIB をポーリングすることができます。Net-SNMP について詳しくは、Net-SNMP の資料を参照してください。

IBM Security QRadar では、構成済みの条件が満たされた場合に SNMP トラップを送信するルール応答を生成するルールを構成できます。QRadar は、SNMP トラップを別のシステムに送信するエージェントの役割をします。

Simple Network Management Protocol (SNMP) トラップは、QRadar が追加処理のために構成済みの SNMP ホストに送信するイベントまたはオフェンス通知です。

カスタム・ルール・ウィザードで SNMP 構成パラメーターをカスタマイズし、カスタム・ルール・エンジンが別の管理用ソフトウェアに送信する SNMP トラップを変更します。QRadar には、2 つのデフォルト・トラップがあります。ただし、カスタム・トラップを追加したり、新しいパラメーターを使用するように既存のトラップを変更することも可能です。

SNMP について詳しくは、Internet Engineering Task Force の Web サイト (http://www.ietf.org/) にアクセスし、検索フィールドに「RFC 1157」と入力してください。

関連概念:

5 ページの『IBM Security QRadar 製品の機能』

IBM Security QRadar 製品資料では、オフェンス、フロー、アセット、ヒストリカル相関などの機能について説明していますが、すべての QRadar 製品でこれらの機能を利用できるわけではありません。使用する製品によっては、説明されている一部の機能をデプロイメントで使用できない場合があります。各製品の機能を確認して、必要な情報を入手してください。

他のシステムに送信される SNMP トラップ情報のカスタマイズ

IBM Security QRadar では、SNMP トラップ・パラメーターを編集して、ルール条件が満たされたときに他の SNMP 管理システムに送信される情報をカスタマイズすることができます。

制約事項: SNMP トラップ・パラメーターがカスタム・ルール・ウィザードに表示されるのは、QRadar システム設定で SNMP が有効になっている場合のみです。

手順

1. SSH を使用して、root ユーザーとして QRadar にログインします。
2. /opt/qradar/conf ディレクトリーに移動し、以下のファイルのバックアップ・コピーを作成します。

- eventCRE.snmp.xml
- offenseCRE.snmp.xml

3. 構成ファイルを編集用に開きます。
   - イベント・ルールの SNMP パラメーターを編集するには、eventCRE.snmp.xml ファイルを開きます。
   - オフェンス・ルールの SNMP パラメーターを編集するには、offenseCRE.snmp.xml ファイルを開きます。
4. <snmp> エレメント内および <creSNMPTrap> エレメントの前に以下のセクションを挿入し、必要に応じてラベルを更新します。

```
<creSNMPResponse name="snmp_response_1">
  <custom name="MyColor">
    <string label="What is your favorite color?"/>
</custom>
  <custom name="MyCategory">
    <list label="Select a category">
      <option label="Label1" value="Category1"/>
      <option label="Label2" value="Category2"/>
    </list>
  </custom>
</creSNMPResponse>
```

5. ファイルを保存して閉じます。
6. /opt/qradar/conf ディレクトリーから /store/configservices/staging/globalconfig ディレクトリーにファイルをコピーします。
7. QRadar インターフェースにログインします。
8. 「管理」タブで、「拡張」 > 「すべての構成のデプロイ」を選択します。

   完全構成をデプロイすると、QRadar によりすべてのサービスが再始動されます。イベントおよびフローに関するデータ収集は、デプロイが完了するまで停止します。

次のタスク

SNMP トラップ出力をカスタマイズします。

SNMP トラップ出力のカスタマイズ

IBM Security QRadar は SNMP を使用して、ルール条件が満たされたときに情報を提供するトラップを送信します。

デフォルトでは、QRadar は QRadar 管理情報ベース (MIB) を使用して、通信ネットワークでデバイスを管理します。ただし、別の MIB に従うように SNMP トラップの出力をカスタマイズすることができます。

手順

1. SSH を使用して、root ユーザーとして QRadar にログインします。
2. /opt/qradar/conf ディレクトリーに移動し、以下のファイルのバックアップ・コピーを作成します。
   - eventCRE.snmp.xml
   - offenseCRE.snmp.xml

3. 構成ファイルを編集用に開きます。
   - イベント・ルールの SNMP パラメーターを編集するには、eventCRE.snmp.xml ファイルを開きます。
   - オフェンス・ルールの SNMP パラメーターを編集するには、offenseCRE.snmp.xml ファイルを開きます。
4. SNMP トラップ通知に使用するトラップを変更するには、適切なトラップ・オブジェクト ID (OID) で以下のテキストを更新します。

   ```
   -<creSNMPTrap version="3" OID="1.3.6.1.4.1.20212.1.1"
   name="eventCRENotification">
   ```

5. 以下の表を参照して、変数バインディング情報を更新してください。

   各変数バインディングは、特定の MIB オブジェクト・インスタンスをその現行値と関連付けます。

表 74. 変数バインディングの値のタイプ

値のタイプ	説明	例
string	英数字 複数の値を構成できます。	
integer32	数値	name="ATTACKER_PORT" type="integer32">%ATTACKER_PORT%
oid	各 SNMP トラップの ID は、MIB 内のオブジェクトに割り当てられます。	OID="1.3.6.1.4.1.20212.2.46"
gauge32	数値範囲	
counter64	定義された最小値から最大値までの範囲内で増分する数値	

6. 値タイプごとに、以下のいずれかのフィールドを含めます。

表 75. 変数バインディングのフィールド

フィールド	説明	例
ネイティブ	これらのフィールドについて詳しくは、/opt/qradar/conf/snmp.help ファイルを参照してください。	**例:** [1]値タイプが ipAddress の場合は、IP アドレスを表す変数を使用する必要があります。ストリング値タイプは、どの形式でも受け入れます。
カスタム	カスタム・ルール・ウィザードで構成したカスタム SNMP トラップ情報	**例:** [1]デフォルトのファイル情報を使用していて、この情報を SNMP トラップに含める必要がある場合は、以下のコードを含めます。 <variableBinding name="My Color Variable Binding" OID="1.3.6.1.4.1.20212.3.1" type="string"> My favorite color is %MyColor%</variableBinding>

表 75. 変数バインディングのフィールド (続き)

フィールド	説明	例
[1]フィールド名をパーセント記号 (%) で囲んでください。パーセント記号内のフィールドは、値タイプと一致していなければなりません。		

7. ファイルを保存して閉じます。
8. /opt/qradar/conf ディレクトリーから /store/configservices/staging/globalconfig ディレクトリーにファイルをコピーします。
9. QRadar インターフェースにログインします。
10. 「管理」タブで、「拡張」 > 「すべての構成のデプロイ」を選択します。

    完全構成をデプロイすると、QRadar によりすべてのサービスが再始動されます。イベントおよびフローに関するデータ収集は、デプロイが完了するまで停止します。

QRadar へのカスタム SNMP トラップの追加

IBM Security QRadar 製品では、カスタム・ルール・ウィザードで SNMP トラップを選択するための新規オプションを作成できます。リスト・ボックスで指定したトラップ名が snmp-master.xml 構成ファイル内に構成されます。

手順

1. SSH を使用して、root ユーザーとして QRadar にログインします。
2. /opt/qradar/conf ディレクトリーに移動します。
3. 新規トラップ用の SNMP 設定ファイルを作成します。

    ヒント: 既存の SNMP 設定ファイルのいずれかをコピーして名前変更し、ファイルに変更を加えます。
4. snmp-master.xml ファイルのバックアップ・コピーを作成します。
5. 編集のために snmp-master.xml ファイルを開きます。
6. 新しい <include> エレメントを追加します。

    <include> エレメントには以下の属性があります。

表 76. <*include*> エレメントの属性

属性	説明
name	リスト・ボックスに表示される
uri	カスタム SNMP 設定ファイルの名前

    例:

```
<include name="Custom_Event_Name" uri="customSNMPdef01.xml"/>
```

    トラップは、snmp-master.xml ファイルにリストされた順序どおりにメニューに表示されます。
7. ファイルを保存して閉じます。

8. /opt/qradar/conf ディレクトリーから /store/configservices/staging/globalconfig ディレクトリーにファイルをコピーします。
9. QRadar インターフェースにログインします。
10. 「管理」タブで、「拡張」 > 「すべての構成のデプロイ」を選択します。

    完全構成をデプロイすると、QRadar によりすべてのサービスが再始動されます。イベントおよびフローに関するデータ収集は、デプロイが完了するまで停止します。

特定のホストへの SNMP トラップの送信

IBM Security QRadar 製品のデフォルトでは、host.conf ファイルで特定されたホストに SNMP トラップが送信されます。 snmp.xml ファイルをカスタマイズして、SNMP トラップを別のホストに送信することができます。

手順

1. SSH を使用して、root ユーザーとして QRadar にログインします。
2. /opt/qradar/conf ディレクトリーに移動し、以下のファイルのバックアップ・コピーを作成します。
   - eventCRE.snmp.xml
   - offenseCRE.snmp.xml
3. 構成ファイルを編集用に開きます。
   - イベント・ルールの SNMP パラメーターを編集するには、eventCRE.snmp.xml ファイルを開きます。
   - オフェンス・ルールの SNMP パラメーターを編集するには、offenseCRE.snmp.xml ファイルを開きます。
4. *<trapConfig>* エレメントを 1 つだけ、*<snmp>* エレメント内の *<creSNMPTrap>* エレメント内および他の子エレメントの前に追加します。

```
<trapConfig>
  <!-- All attribute values are default -->
   <snmpHost snmpVersion="3" port="162" retries="2" timeout="500">HOST
   </snmpHost>
  <!-- Community String for Version 2 -->
   <communityString>COMMUNITY_STRING</communityString>
  <!-- authenticationProtocol (MD5 or SHA)securityLevel (AUTH_PRIV, AUTH_NOPRIV
  or NOAUTH_PRIV) -->
   <authentication authenticationProtocol="MD5"securityLevel="AUTH_PRIV">
    AUTH_PASSWORD
   </authentication>
  <!-- decryptionProtocol (DES, AES128, AES192 or AES256) -->
   <decryption decryptionProtocol="AES256">
     DECRYPTIONPASSWORD
   </decryption>
  <!-- SNMP USER-->
   <user> SNMP_USER </user>
 </trapConfig>
```

5. 以下の表を参照して、属性を更新してください。

表 77. *<trapConfig>* エレメント内で更新する属性値

エレメント	説明
</snmpHost>	SNMP トラップの送信先の新規ホスト。 <snmpHost> エレメントの snmpVersion 属性値は 2 または 3 でなければなりません。
<communityString>	ホストのコミュニティー・ストリング。
<authentication>	ホストの認証プロトコル、セキュリティー・レベル、パスワード。
<decryption>	ホストの暗号化解除プロトコルおよびパスワード。
<user>	SNMP ユーザー

6. ファイルを保存して閉じます。
7. /opt/qradar/conf ディレクトリーから /store/configservices/staging/globalconfig ディレクトリーにファイルをコピーします。
8. QRadar インターフェースにログインします。
9. 「管理」タブで、「拡張」 > 「すべての構成のデプロイ」を選択します。

   完全構成をデプロイすると、QRadar によりすべてのサービスが再始動されます。イベントおよびフローに関するデータ収集は、デプロイが完了するまで停止します。

第 23 章 機密データの保護

IBM Security QRadar では、機密情報や個人情報への無許可アクセスを防止するために、データ難読化プロファイルを構成します。

データ難読化 とは、QRadar ユーザーに対しデータを戦略的に非表示にするプロセスです。カスタム・プロパティー、正規化されたプロパティー (ユーザー名など) やペイロードのコンテンツ (クレジット・カード番号や社会保障番号など) を非表示にすることができます。

データ難読化プロファイル内の式が、ペイロードや正規化されたプロパティーに対して評価されます。データが難読化式と一致した場合、そのデータは QRadar で非表示になります。データベースを直接照会しようとするユーザーには、機密データが表示されません。データを元の形式に戻す (難読化解除する) 必要があります。このためには、データ難読化プロファイルの作成時に生成された秘密鍵をアップロードします。

QRadar が非表示のデータ値の相関を確実にとることができるようにするため、難読化プロセスは決定論的です。データ値が検出されるたびに、同一の文字セットが表示されます。

関連概念:

5 ページの『IBM Security QRadar 製品の機能』
IBM Security QRadar 製品資料では、オフェンス、フロー、アセット、ヒストリカル相関などの機能について説明していますが、すべての QRadar 製品でこれらの機能を利用できるわけではありません。使用する製品によっては、説明されている一部の機能をデプロイメントで使用できない場合があります。各製品の機能を確認して、必要な情報を入手してください。

データ難読化の仕組み

IBM Security QRadar デプロイメントでデータ難読化を構成する場合は、新規および既存のオフェンス、アセット、ルール、およびログ・ソース拡張に対してデータ難読化がどのように機能するかを理解しておく必要があります。

既存のイベント・データ

データ難読化プロファイルを有効にすると、QRadar が受信する各イベントのデータがマスクされます。データ難読化を構成する前にアプライアンスが受信したイベントは、難読化されていない状態のままとなります。以前のイベント・データはマスクされず、ユーザーはその情報を表示することができます。

アセット

データ難読化を構成すると、アセット・モデルでマスクされたデータが蓄積されますが、既存のアセット・モデル・データはマスクされないままとなります。

難読化された情報が、マスクされていないデータを使用してトレースされないようにするには、アセット・モデル・データをパージしてマスクされていないデータを削除します。QRadar によって、アセット・データベースに難読化された値が再入力されます。

オフェンス

それまでマスクされていなかったデータがオフェンスにより表示されることのないようにするには、SIM モデルをリセットして既存のオフェンスをすべて閉じます。詳しくは、 82 ページの『SIM のリセット』を参照してください。

ルール

以前にマスクが解除されたデータに依存するルールを更新する必要があります。例えば、ユーザー名が難読化されると、特定のユーザー名を基準とするルールは作動しなくなります。

ログ・ソース拡張

イベント・ペイロードのフォーマットを変更するログ・ソース拡張が原因で、データ難読化に問題が生じる場合があります。

データ難読化プロファイル

データ難読化プロファイルには、マスク対象のデータに関する情報が含まれています。また、このプロファイルによって、データの復号に必要な鍵ストアが追跡されます。

有効化されたプロファイル
: プロファイルは、難読化するデータが式によって正しく特定されることが確実である場合にのみ有効化してください。データ難読化プロファイルを有効化する前に正規表現をテストする場合は、正規表現ベースのカスタム・プロパティーを作成できます。

  有効化されたプロファイルは、プロファイル内の有効な式で定義されたとおりに、データの難読化をただちに開始します。有効化されたプロファイルは自動的にロックされます。有効化されたプロファイルを無効化または変更できるのは、秘密鍵を持つユーザーだけです。

  難読化したデータを難読化プロファイルまでたどれるようにするために、一度有効化したプロファイルは、無効化しても削除できません。

ロックされたプロファイル
: プロファイルは、有効化すると自動的にロックされますが、手動でロックすることもできます。

  プロファイルをロックすると、以下のことが制限されます。

  - 編集できなくなります。
  - 有効化も無効化できなくなります。プロファイルを変更するには、鍵ストアを提供してプロファイルをアンロックする必要があります。
  - 削除できなくなります。アンロックしても同様です。

- ロックされたプロファイルで鍵ストアを使用すると、同じ鍵ストアを使用する他のすべてのプロファイルが自動的にロックされます。

プロファイルがロックまたはアンロックされる例を以下の表に示します。

表 *78.* ロックされたプロファイルの例

シナリオ	結果
プロファイル A がロックされている。このプロファイルは鍵ストア A を使用して作成されている。 プロファイル B も鍵ストア A を使用して作成されている。	プロファイル B が自動的にロックされます。
プロファイル A が作成され、有効化された。	プロファイル A が自動的にロックされます。
プロファイル A、プロファイル B、およびプロファイル C が現在ロックされている。いずれも鍵ストア A を使用して作成されている。 プロファイル B が選択されて「ロック/アンロック」がクリックされた。	プロファイル A、プロファイル B、プロファイル C がすべてアンロックされます。

データ難読化式

データ難読化式は、非表示にするデータを特定します。フィールド・ベースのプロパティーに基づくデータ難読化式を作成するか、または正規表現を使用することができます。

フィールド・ベースのプロパティー

フィールド・ベースのプロパティーは、ユーザー名、グループ名、ホスト名、および NetBIOS 名を非表示にする場合に使用します。フィールド・ベースのプロパティーを使用する式では、データ・ストリングのすべてのインスタンスが難読化されます。データは、そのログ・ソース、ログ・ソース・タイプ、イベント名、またはイベント・カテゴリーに関係なく非表示にされます。

同じデータ値が複数のフィールドに存在する場合は、4 つのフィールドのうち 1 つのみを難読化するようにプロファイルを構成していても、すべてのフィールドでデータが難読化されます。例えば、ホスト名が `IBMHost` でありグループ名も `IBMHost` である場合は、データ難読化プロファイルがホスト名のみを難読化するように構成されている場合でも、ホスト名フィールドとグループ名フィールドの両方で値 `IBMHost` が難読化されます。

正規表現

正規表現は、ペイロード内の 1 つのデータ・ストリングを難読化する場合に使用します。データが非表示になるのは、そのデータが式に定義されたログ・ソース、ログ・ソース・タイプ、イベント名、またはカテゴリーに一致した場合のみです。

上位カテゴリーと下位カテゴリーを使用して、フィールド・ベースのプロパティーよりも特定的な正規表現を作成できます。例えば、以下の正規表現パターンを使用してユーザー名を解析できます。

表 79. 正規表現によるユーザー名の解析

regex パターンの例	マッチング
usrName=([0-9a-zA-Z]([-.¥w]*[0-9a-zA-Z])*@([0-9 a-zA-Z][-¥w]*[0-9a-zA-Z]¥.)+[a-zA-Z]{2,20})$	john_smith@IBM.com, jon@ibm.com, jon@us.ibm.com
usrName=(^([¥w]+[^¥W])([^¥W]¥.?)([¥w]+[^¥W]$))	john.smith, John.Smith, john, jon_smith
usrName=^([a-zA-Z])[a-zA-Z_-]*[¥w_-]*[¥S]$\|^([a -zA-Z])[0-9_-]*[¥S]$|^[a-zA-Z]*[¥S]$	johnsmith, Johnsmith123, john_smith123, john123_smith, john-smith
usrName=(/S+)	等号 (=) の後の空白以外のものとマッチングします。この正規表現は特定的ではないため、システム・パフォーマンスに問題が生じる可能性があります。
msg=([0-9a-zA-Z]([-.¥w]*[0-9a-zA-Z]))*@¥b(([01] ?¥d?¥d|2[0-4]¥d|25[0-5])¥.){3}([01]?¥d?¥d|2[0-4]¥d|25[0-5])¥b	IP アドレスを持つユーザーをマッチングします。例: john.smith@1.1.1.1
src=¥b(([01]?¥d?¥d|2[0-4]¥d|25[0-5])¥.){3}([01] ?¥d?¥d|2[0-4]¥d|25[0-5])¥b	IP アドレス・フォーマットをマッチングします。
host=^(([a-zA-Z0-9]|[a-zA-Z0-9][a-zA-Z0-9¥-]*[a -zA-Z0-9])¥.)*([A-Za-z0-9]|[A-Za-z0-9][A-Za-z0- 9¥-]*[A-Za-z0-9])$	hostname.ibm.com、 hostname.co.uk

シナリオ: ユーザー名の難読化

あなたは IBM Security QRadar 管理者です。組織と労働組合との間に、個人を特定できるすべての情報は QRadar のユーザーに対して非表示にしなければならないという合意があります。すべてのユーザー名を非表示にするように QRadar を構成するとします。

「管理」タブの「データ難読化管理」機能を使用して、データを非表示にするように QRadar を構成します。

1. データ難読化プロファイルを作成し、システムで生成された秘密鍵をダウンロードします。その鍵をセキュアな場所に保存します。
2. 非表示にするデータをターゲットとしたデータ難読化式を作成します。
3. システムがデータの難読化を開始するようにプロファイルを有効にします。
4. QRadar でデータを読み取るために、データを難読化解除するための秘密鍵をアップロードします。

データ難読化プロファイルの作成

IBM Security QRadar では、データ難読化プロファイルを使用して、マスクするデータを特定するとともに、データのマスクを解除する際に正しい鍵ストアが使用されていることを確認します。

このタスクについて

新しい鍵ストアを作成するプロファイルを作成するか、既存の鍵ストアを使用することができます。鍵ストアを作成する場合は、鍵ストアをダウンロードして安全な場所に保管する必要があります。鍵ストアをローカル・システムから削除し、マスクが解除されたデータを表示する権限を持つユーザーのみがアクセスできる場所に保管します。

データ・アクセスをユーザー・グループ別に制限したい場合は、別々の鍵ストアを使用する複数のプロファイルを構成すると便利です。例えば、あるユーザー・グループにはユーザー名を表示し、別のユーザー・グループにはホスト名を表示する場合は、別々の鍵ストアを使用する 2 つのプロファイルを作成します。

手順

1. 「管理」タブをクリックします。
2. ナビゲーション・メニューで、「データ・ソース」 > 「データ難読化管理」をクリックします。
3. 新しいプロファイルを作成する場合は、「追加」をクリックし、プロファイルの固有の名前と説明を入力します。
4. このプロファイルの新しい鍵ストアを作成するには、以下の手順を実行します。
   a. 「システム生成鍵ストア」をクリックします。
   b. 「プロバイダー」リスト・ボックスで、「**IBMJCE**」を選択します。
   c. 「アルゴリズム」リスト・ボックスで「**JCE**」を選択し、512 ビットと 1024 ビットのどちらの暗号鍵を生成するかを選択します。 「鍵ストア証明書 **CN**」ボックスに、QRadar サーバーの完全修飾ドメイン名が自動的に入力されます。
   d. 「鍵ストアのパスワード」ボックスに、鍵ストアのパスワードを入力します。 鍵ストアの保全性を保つために、鍵ストアのパスワードが必要です。パスワードは 8 文字以上の長さでなければなりません。
   e. 「鍵ストアのパスワードの検証」に、もう一度パスワードを入力します。
5. プロファイルで既存の鍵ストアを使用する場合は、以下の手順を実行します。
   a. 「鍵ストアのアップロード」をクリックします。
   b. 「参照」をクリックし、鍵ストア・ファイルを選択します。
   c. 「鍵ストアのパスワード」ボックスに、鍵ストアのパスワードを入力します。
6. 「送信 **(Submit)**」をクリックします。
7. 鍵ストアをダウンロードします。 システムから鍵ストアを削除し、安全な場所に保管します。

次のタスク

非表示にするデータをターゲットとするデータ難読化式を作成します。

データ難読化式の作成

データ難読化プロファイルでは、式を使用して非表示にするデータを指定します。式では、フィールド・ベースのプロパティーまたは正規表現のいずれかを使用できます。

このタスクについて

式の作成後にタイプを変更することはできません。例えば、プロパティー・ベースの式を作成した後に、その式を正規表現に変更することはできません。

正規化された数字フィールド (ポート番号や IP アドレスなど) は難読化できません。

同じデータを難読化する式が複数あると、データが 2 回難読化されることになります。複数回難読化されたデータを復号するには、難読化処理で使用された各鍵ストアを、難読化が行われた順序で適用しなければなりません。

手順

1. 「管理」タブをクリックします。
2. ナビゲーション・メニューで、「データ・ソース」 > 「データ難読化管理」をクリックします。
3. 構成するプロファイルをクリックし、「内容の表示」をクリックします。 ロックされているプロファイルは構成できません。
4. 新しいデータ難読化式を作成するには、「追加」をクリックし、プロファイルの固有の名前と説明を入力します。
5. 「有効」チェック・ボックスを選択してプロファイルを有効にします。
6. フィールド・ベースの式を作成する場合は、「フィールド・ベース」をクリックし、難読化するフィールド・タイプを選択します。
7. 正規表現を作成する場合は、「正規表現」をクリックし、正規表現のプロパティーを構成します。
8. 「保存」をクリックします。

コンソールに表示できるようにするためのデータの難読化解除

IBM Security QRadar システムでデータ難読化が構成されている場合は、アプリケーション全体でデータがマスクされて表示されます。データを難読化解除して表示できるようにするには、対応する鍵ストアとパスワードの両方が必要です。

始める前に

データを難読化解除するには、事前に秘密鍵とその鍵のパスワードを保有している必要があります。秘密鍵はローカル・コンピューター上に存在している必要があります。

このタスクについて

難読化データを表示するには、事前に秘密鍵をアップロードする必要があります。アップロードされた鍵は、現行セッションの期間にわたってシステム上で使用可能になります。QRadar からログアウトするか、QRadar コンソール でキャッシュが

クリアされるか、または非アクティブな状態が長時間続いた場合は、セッションが終了します。セッションが終了すると、前のセッションでアップロードされた秘密鍵は表示されなくなります。

QRadar は現行セッションで使用可能な鍵を使用して、自動的にデータを難読化解除します。自動難読化解除を有効にすると、データを表示するたびに「難読化セッション鍵」ウィンドウで繰り返し秘密鍵を選択する必要がなくなります。自動難読化解除は、現在のセッションが終了すると自動的に無効になります。

手順

1. 「イベントの詳細」ページで、難読化解除するデータを見つけます。
2. ID ベースのデータを難読化解除するには、以下の手順に従います。
   a. 難読化解除するデータの横にあるロック・アイコンをクリックします。
   b. 「鍵のアップロード」セクションで、「ファイルの選択」をクリックし、アップロードする鍵ストアを選択します。
   c. 「パスワード」ボックスに、鍵ストアに対応するパスワードを入力します。
   d. 「アップロード」をクリックします。

      「難読化解除」ウィンドウに、イベント・ペイロード、鍵ストアに関連付けられているプロファイル名、難読化されたテキスト、および難読化解除されたテキストが表示されます。
   e. オプション: 「自動難読化解除の切り替え」をクリックして自動難読化解除を有効にします。

      自動難読化解除の設定を切り替えた場合は、変更を反映させるために、ブラウザー・ウィンドウを最新表示してイベントの詳細ページを再ロードする必要があります。
3. ID ベースではないペイロード・データを難読化解除するには、以下の手順に従います。
   a. 「イベントの詳細」ページのツールバーで、「難読化」 > 「難読化解除鍵」をクリックします。
   b. 「鍵のアップロード」セクションで、「ファイルの選択」をクリックし、アップロードする秘密鍵を選択します。
   c. 「パスワード」ボックスに、秘密鍵に一致するパスワードを入力して「アップロード」をクリックします。
   d. 「ペイロード情報」ボックスで難読化テキストを選択し、クリップボードにコピーします。
   e. 「イベントの詳細」ページのツールバーで、「難読化」 > 「難読化解除」をクリックします。
   f. ダイアログ・ボックスに難読化テキストを貼り付けます。
   g. ドロップダウン・リストから難読化プロファイルを選択し、「難読化解除」をクリックします。

以前のリリースで作成された難読化式の編集または無効化

IBM Security QRadar V7.2.6 にアップグレードすると、以前のリリースで作成されたデータ難読化式が自動的に継承されてデータの難読化に使用されます。これらの式は、**AutoGeneratedProperty** という名前の、1 つのデータ難読化プロファイルに含まれています。

以前のバージョンで作成されたデータ難読化式は、表示することはできますが、編集することも無効化することもできません。これらの式を手動で無効化し、修正した式を含むデータ難読化プロファイルを作成する必要があります。

このタスクについて

以前の式を無効化するには、式の属性を定義する `xml` 構成ファイルを編集する必要があります。その後に `obfuscation_updater.sh` スクリプトを実行して無効化できます。

同じデータを難読化する式を新たに作成する場合は、必ず以前の式を無効化してください。同じデータを難読化する式が複数あると、データが 2 回難読化されることになります。複数回難読化されたデータを復号するには、難読化処理で使用された各鍵ストアを、難読化が行われた順序で適用しなければなりません。

手順

1. SSH を使用して、QRadar コンソールに root ユーザーとしてログインします。
2. 式を構成するときに作成した難読化式の `.xml` 構成ファイルを編集します。
3. 無効化する式ごとに、**`Enabled`** 属性を `false` に変更します。
4. 式を無効化するために、以下のコマンドを入力して `obfuscation_updater.sh` スクリプトを実行します。

   ```
   obfuscation_updater.sh [-p <path_to_private_key>] [-e
   <path_to_obfuscation_xml_config_file>]
   ```

   `obfuscation_updater.sh` スクリプトは `/opt/qradar/bin` ディレクトリーにありますが、QRadar コンソール上の任意のディレクトリーから実行できます。

次のタスク

QRadar で直接データを難読化し、難読化式を管理するため、 データ難読化プロファイルを作成します。

第 24 章 ログ・ファイル

IBM Security QRadar で実行される操作は、追跡のためにログ・ファイルに記録されます。ログ・ファイルは、製品を操作するときに発生するアクティビティーを記録することにより、問題のトラブルシューティングに役立てることができます。

次のログ・ファイルは、問題が発生したときにそれを特定して解決するのに役立ちます。

- /var/log/qradar.log
- /var/log/qradar.error
- /var/log/qradar-sql.log
- /opt/tomcat6/logs/catalina.out
- /var/log/qflow.debug

QRadar のログ・ファイルを収集して、後で確認する場合は、 81 ページの『ログ・ファイルの収集』を参照してください。

関連概念:

5 ページの『IBM Security QRadar 製品の機能』
IBM Security QRadar 製品資料では、オフェンス、フロー、アセット、ヒストリカル相関などの機能について説明していますが、すべての QRadar 製品でこれらの機能を利用できるわけではありません。使用する製品によっては、説明されている一部の機能をデプロイメントで使用できない場合があります。各製品の機能を確認して、必要な情報を入手してください。

監査ログ

IBM Security QRadar ユーザーにより行われた変更は監査ログに記録されます。

監査ログを参照して、QRadar に対する変更と、設定を変更したユーザーをモニターすることができます。

すべての監査ログは、プレーン・テキストで保管され、監査ログ・ファイルが 200 MB に達するとアーカイブおよび圧縮されます。現行のログ・ファイルの名前は audit.log です。このファイルのサイズが 200 MB に到達すると、ファイルが圧縮されてファイル名が audit.1.gz に変更されます。ログ・ファイルがアーカイブされるたびに、ファイル名の番号が 1 ずつ増えていきます。QRadar には、最大で 50 個のアーカイブ・ログ・ファイルが保管されます。

監査ログ・ファイルの表示

セキュア・シェル (SSH) を使用して IBM Security QRadar システムにログインし、システムへの変更をモニターします。

このタスクについて

「ログ・アクティビティー」タブを使用して、正規化された監査ログ・イベントを表示できます。

監査メッセージ (日付、時刻、ホスト名は除外) の最大サイズは 1024 文字です。

ログ・ファイルの各エントリーは以下の形式を使用して表示されます。

<date_time> <host name> <user>@<IP address> (thread ID) [<category>] [<sub-category>] [<action>] <payload>

次の表で、ログ・ファイル・フォーマットのオプションについて説明します。

表 *80.* ログ・ファイル・フォーマットの各部分についての説明

ファイル・フォーマットの部分	説明
date_time	次の形式の、アクティビティーの日付と時刻。Month Date HH:MM:SS
host name	このアクティビティーがログに記録されたコンソールのホスト名。
user	設定を変更したユーザーの名前。
IP address	設定を変更したユーザーの IP アドレス。
(thread ID)	このアクティビティーをログに記録した Java™ スレッドの ID。
category	このアクティビティーの上位カテゴリー。
sub-categor	このアクティビティーの下位カテゴリー。
action	発生したアクティビティー。
payload	変更のあった、完全なレコード。ユーザー・レコードまたはイベント・ルールを含むことがあります。

手順

1. SSH を使用して、root ユーザーとして QRadar にログインします。
2. ユーザー名: `root`
3. パスワード: *password*
4. 以下のディレクトリーに移動します。

   ```
   /var/log/audit
   ```
5. 監査ログ・ファイルを開いて表示します。

ログに記録されるアクション

`/var/log/audit` ディレクトリー内の IBM Security QRadar 監査ログ・ファイルのコンテンツを理解します。監査ログ・ファイルには、ログに記録されたアクションが含まれます。

以下のリストで、監査ログ・ファイル内のアクションのカテゴリーを説明します。

管理者認証

- 管理コンソールにログインする。
- 管理コンソールからログアウトする。

アセット

- 特定の 1 つのアセットを削除する。
- すべてのアセットを削除する。

監査ログ・アクセス

監査の上位イベント・カテゴリーを持つイベントを含んだ検索。

バックアップとリカバリー

- 構成を編集する。
- バックアップを開始する。
- バックアップを完了する。
- バックアップが失敗する。
- バックアップを削除する。
- バックアップを同期する。
- バックアップを取り消す。
- リストアを開始する。
- バックアップをアップロードする。
- 無効なバックアップをアップロードする。
- リストアを開始する。
- バックアップをパージする。

チャート構成

フロー・チャートまたはイベント・チャートの構成を保存する。

コンテンツ・マネジメント

- コンテンツのエクスポートが開始された。
- コンテンツのエクスポートが完了した。
- コンテンツのインポートが開始された。
- コンテンツのインポートが完了した。
- コンテンツの更新が開始された。
- コンテンツの更新が完了した。
- コンテンツの検索が開始された。
- アプリケーションが追加された。
- アプリケーションが変更された。
- カスタム・アクションが追加された。
- カスタム・アクションが変更された。
- Ariel プロパティーが追加された。
- Ariel プロパティーが変更された。
- Ariel プロパティー式が追加された。
- Ariel プロパティー式が変更された。
- CRE ルールが追加された。

- CRE ルールが変更された。
- ダッシュボードが追加された。
- ダッシュボードが変更された。
- デバイス拡張が追加された。
- デバイス拡張が変更された。
- デバイス拡張の関連付けが変更された。
- グループ化が追加された。
- グループ化が変更された。
- ヒストリカル相関プロファイルが追加された。
- ヒストリカル相関プロファイルが変更された。
- QID マップ項目が追加された。
- QID マップ項目が変更された。
- リファレンス・データが作成された。
- リファレンス・データが更新された。
- セキュリティー・プロファイルが追加された。
- セキュリティー・プロファイルが変更された。
- センサー・デバイスが追加された。
- センサー・デバイスが変更された。

カスタム・プロパティー

- カスタム・イベント・プロパティーを追加する。
- カスタム・イベント・プロパティーを編集する。
- カスタム・イベント・プロパティーを削除する。
- カスタム・フロー・プロパティーを編集する。
- カスタム・フロー・プロパティーを削除する。

カスタム・プロパティーの式

- カスタム・イベント・プロパティーの式を追加する。
- カスタム・イベント・プロパティーの式を編集する。
- カスタム・イベント・プロパティーの式を削除する。
- カスタム・フロー・プロパティーの式を追加する。
- カスタム・フロー・プロパティーの式を編集する。
- カスタム・フロー・プロパティーの式を削除する。

フロー・ソース

- フロー・ソースを追加する。
- フロー・ソースを編集する。
- フロー・ソースを削除する。

グループ

- グループを追加する。
- グループを削除する。
- グループを編集する。

ヒストリカル相関

- ヒストリカル相関プロファイルを追加する。
- ヒストリカル相関プロファイルを削除する。
- ヒストリカル相関プロファイルを変更する。
- ヒストリカル相関プロファイルを有効にする。
- ヒストリカル相関プロファイルを無効にする。
- ヒストリカル相関プロファイルが実行中である。
- ヒストリカル相関プロファイルがキャンセルされた。

ライセンス

- ライセンス・キーを追加する。
- ライセンス・キーを削除する。
- ライセンス・プールの割り振りを削除する。
- ライセンス・プールの割り振りを更新する。

ログ・ソース拡張

- ログ・ソース拡張を追加する。
- ログ・ソース拡張を編集する。
- ログ・ソース拡張を削除する。
- ログ・ソース拡張をアップロードする。
- ログ・ソース拡張を正常にアップロードする。
- 無効なログ・ソース拡張をアップロードする。
- ログ・ソース拡張をダウンロードする。
- ログ・ソース拡張を報告する。
- デバイスまたはデバイス・タイプへのログ・ソースの関連付けを変更する。

オフェンス

- オフェンスを非表示にする。
- オフェンスをクローズする。
- すべてのオフェンスをクローズする。
- 宛先のメモを追加する。
- ソースのメモを追加する。
- ネットワークのメモを追加する。
- オフェンスのメモを追加する。
- オフェンスをクローズする理由を追加する。
- オフェンスをクローズする理由を編集する。

プロトコル構成

- プロトコル構成を追加する。
- プロトコル構成を削除する。
- プロトコル構成を編集する。

QIDmap

- QID マップ・エントリーを追加する。
- QID マップ・エントリーを編集する。

IBM Security QRadar Vulnerability Manager

- スキャナーのスケジュールを作成する。
- スキャナーのスケジュールを更新する。
- スキャナーのスケジュールを削除する。
- スキャナーのスケジュールを開始する。
- スキャナーのスケジュールを一時停止する。
- スキャナーのスケジュールを再開する。

リファレンス・セット

- リファレンス・セットを作成する。
- リファレンス・セットを編集する。
- リファレンス・セットのエレメントをパージする。
- リファレンス・セットを削除する。
- リファレンス・セット・エレメントを追加する。
- リファレンス・セット・エレメントを削除する。
- すべてのリファレンス・セット・エレメントを削除する。
- リファレンス・セット・エレメントをインポートする。
- リファレンス・セット・エレメントをエクスポートする。

レポート

- テンプレートを追加する。
- テンプレートを削除する。
- テンプレートを編集する。
- レポートを生成する。
- レポートを削除する。
- 生成されたコンテンツを削除する。
- 生成されたレポートを表示する。
- 生成されたレポートを E メールで送信する。

保存バケット

- バケットを追加する。
- バケットを削除する。
- バケットを編集する。
- バケットを有効または無効にする。

root ログイン

- QRadar に root ユーザーとしてログインする。
- QRadar から root ユーザーとしてログアウトする。

ルール

- ルールを追加する。
- ルールを削除する。

- ルールを編集する。

スキャナー

- スキャナーを追加する。
- スキャナーを削除する。
- スキャナーを編集する。

スキャナーのスケジュール

- スケジュールを追加する。
- スケジュールを編集する。
- スケジュールを削除する。

セッションの認証

- 管理セッションを作成する。
- 管理セッションを終了する。
- 無効な認証セッションを拒否する。
- セッション認証を有効期限切れにする。
- 認証セッションを作成する。
- 認証セッションを終了する。

SIM SIM モデルをクリーンアップする。

ストア・アンド・フォワード

- ストア・アンド・フォワード・スケジュールを追加する。
- ストア・アンド・フォワード・スケジュールを編集する。
- ストア・アンド・フォワード・スケジュールを削除する。

Syslog 転送

- Syslog 転送を追加する。
- Syslog 転送を削除する。
- Syslog 転送を編集する。

システム管理

- システムをシャットダウンする。
- システムを再始動する。

ユーザー・アカウント

- アカウントを追加する。
- アカウントを編集する。
- アカウントを削除する。

ユーザー認証

- ユーザー・インターフェースにログインする。
- ユーザー・インターフェースからログアウトする。

Ariel のユーザー認証

- ログイン試行を拒否する。
- Ariel プロパティーを追加する。

- Ariel プロパティーを削除する。
- Ariel プロパティーを編集する。
- Ariel プロパティー拡張を追加する。
- Ariel プロパティー拡張を削除する。
- Ariel プロパティー拡張を編集する。

ユーザー・ロール

- ロールを追加する。
- ロールを編集する。
- ロールを削除する。

VIS

- 新規ホストをディスカバーする。
- 新規オペレーティング・システムをディスカバーする。
- 新規ポートをディスカバーする。
- 新たな脆弱性をディスカバーする。

第 25 章 イベント・カテゴリー

イベント・カテゴリーは、IBM Security QRadar による処理用に、着信イベントをグループ化するために使用されます。イベント・カテゴリーは検索可能で、ネットワークのモニターに役立ちます。

ネットワークで発生するイベントは、上位カテゴリーと下位カテゴリーに集約されます。各上位カテゴリーには、下位カテゴリーおよびそれに関連する重大度レベルと ID 番号が含まれます。

イベントに割り当てられる重大度レベルを検討し、企業ポリシーのニーズに合うように調整できます。

上位および下位のイベント・カテゴリー ID を使用して AQL 照会を実行できます。関連するカテゴリー名のカテゴリー ID は、イベント・カテゴリー・テーブルから取得できます。

例えば、QRadar でアプリケーションを開発する場合、コマンド・ラインで以下の照会に類似する AQL 検索を実行して、Ariel からデータを収集できます。

```
select qidname(qid) as 'Event', username as 'Username', devicetime as
'Time' from events where '<high-level category ID>' and '<Low-level
category ID>' and LOGSOURCENAME(logsourceid) like "%Low-level category
name%" last 3 days
```

関連概念:

5 ページの『IBM Security QRadar 製品の機能』
IBM Security QRadar 製品資料では、オフェンス、フロー、アセット、ヒストリカル相関などの機能について説明していますが、すべての QRadar 製品でこれらの機能を利用できるわけではありません。使用する製品によっては、説明されている一部の機能をデプロイメントで使用できない場合があります。各製品の機能を確認して、必要な情報を入手してください。

上位イベント・カテゴリー

IBM Security QRadar ログ・ソースのイベントは、上位カテゴリーにグループ化されます。各イベントは特定の上位カテゴリーに割り当てられます。

受信イベントをカテゴリー化することにより、データの検索が容易になります。

以下の表で、上位イベント・カテゴリーについて説明します。

表 *81.* 上位イベント・カテゴリー

カテゴリー	カテゴリー **ID**	説明
361 ページの『スキャン行為』	1000	ネットワーク・リソースの識別に使用されるスキャンなどの手法に関連したイベント (ネットワークやホストのポート・スキャンなど)

表 *81.* 上位イベント・カテゴリー *(*続き*)*

カテゴリー	カテゴリー **ID**	説明
363 ページの『DoS』	2000	サービスやホストに対するサービス妨害 (DoS) 攻撃または分散型サービス妨害 (DDoS) 攻撃に関連したイベント (ブルート・フォース・ネットワーク DoS 攻撃など)。
367 ページの『認証』	3000	認証の制御、グループ、または特権の変更に関連したイベント (ログインやログアウトなど)。
378 ページの『アクセス』	4000	ネットワーク・リソースへのアクセス試行によるイベント (ファイアウォールのアクセスや拒否など)。
381 ページの『エクスプロイト (Exploit)』	5000	アプリケーションのエクスプロイトとバッファー・オーバーフローの試行に関連したイベント (バッファー・オーバーフローや Web アプリケーションのエクスプロイトなど)。
384 ページの『マルウェア』	6000	ウィルス、トロイの木馬、バックドア攻撃、または他の形式の悪意のあるソフトウェアに関連したイベント。マルウェア・イベントには、ウィルス、トロイの木馬、悪意のあるソフトウェア、またはスパイウェアなどが含まれます。
385 ページの『疑わしいアクティビティー』	7000	脅威の性質は不明ですが、疑わしい振る舞いです。脅威には、回避的な手法 (パケット・フラグメント化や既知の侵入検知システム (IDS) など) を潜在的に示すプロトコル・アノマリなどが含まれます。
391 ページの『システム』	8000	システム変更、ソフトウェア・インストール、または状況メッセージに関連したイベント。
397 ページの『ポリシー』	9000	企業のポリシー違反または誤用に関するイベント。
399 ページの『不明』	10000	システム上の不明なアクティビティーに関連したイベント。
400 ページの『CRE』	12000	オフェンスルールまたはイベントルールから生成されたイベント。
401 ページの『潜在的エクスプロイト』	13000	潜在的なアプリケーションのエクスプロイトとバッファー・オーバーフローの試行に関連したイベント。
フロー	14000	フロー・アクションに関連したイベント。
404 ページの『ユーザー定義』	15000	ユーザー定義オブジェクトに関連したイベント。
407 ページの『SIM 監査』	16000	コンソール機能および管理機能とのユーザーの対話に関連したイベント。
409 ページの『VIS ホスト・ディスカバリー』	17000	VIS コンポーネントがディスカバーするホスト、ポート、または脆弱性に関連したイベント。

表 *81.* 上位イベント・カテゴリー *(*続き*)*

カテゴリー	カテゴリー **ID**	説明
409 ページの『アプリケーション』	18000	アプリケーション・アクティビティーに関連したイベント。
441 ページの『監査』	19000	監査アクティビティーに関連したイベント。
446 ページの『リスク』	20000	IBM Security QRadar Risk Manager のリスク・アクティビティーに関連したイベント。
448 ページの『リスク・マネージャー監査』	21000	QRadar Risk Manager の監査アクティビティーに関連したイベント。
449 ページの『制御』	22000	ハードウェア・システムに関連したイベント。
451 ページの『アセット・プロファイラー』	23000	アセット・プロファイルに関連したイベント。
センス	24000	UBA に関連したイベント。

スキャン行為

スキャン行為カテゴリーには、ネットワーク・リソースの識別に使用されるスキャンなどの手法に関連したイベントが含まれます。

以下の表で、スキャン行為カテゴリーの下位イベント・カテゴリーおよび関連する重大度レベルについて説明します。

表 *82.* スキャン行為イベント・カテゴリーの下位カテゴリーおよび重大度レベル

下位イベント・カテゴリー	カテゴリー **ID**	説明	重大度レベル **(0** から **10** まで**)**
不明な調査の形式 (Unknown Form of Recon)	1001	不明な形式のスキャン行為。	2
アプリケーション照会 (Application Query)	1002	システム上のアプリケーションに対するスキャン行為。	3
ホスト照会 (Host Query)	1003	ネットワーク内のホストに対するスキャン行為。	3
ネットワーク・スイープ (Network Sweep)	1004	ネットワークに対するスキャン行為。	4
メール・スキャン行為 (Mail Reconnaissance)	1005	メール・システムのスキャン行為。	3
Windows スキャン行為 (Windows Reconnaissance)	1006	Windows オペレーティング・システムに対するスキャン行為。	3

表 82. スキャン行為イベント・カテゴリーの下位カテゴリーおよび重大度レベル (続き)

下位イベント・カテゴリー	カテゴリー ID	説明	重大度レベル (0 から 10 まで)
ポート・マップ/RPC 要求	1007	ポート・マップまたは RPC 要求についてのスキャン行為。	3
ホスト・ポートのスキャン (Host Port Scan)	1008	ホスト・ポートで発生したスキャンを示します。	4
RPC ダンプ (RPC Dump)	1009	リモート・プロシージャー・コール (RPC) 情報が削除されたことを示します。	3
DNS スキャン行為 (DNS Reconnaissance)	1010	DNS サーバーのスキャン行為。	3
その他のスキャン行為イベント (Misc Reconnaissance Event)	1011	その他のスキャン行為イベント。	2
Web スキャン行為 (Web Reconnaissance)	1012	ネットワーク上の Web スキャン行為	3
データベース・スキャン行為 (Database Reconnaissance)	1013	ネットワーク上のデータベース・スキャン行為	3
ICMP スキャン行為 (ICMP Reconnaissance)	1014	ICMP トラフィックのスキャン行為。	3
UDP スキャン行為 (UDP Reconnaissance)	1015	UDP トラフィックのスキャン行為。	3
SNMP スキャン行為 (SNMP Reconnaissance)	1016	SNMP トラフィックのスキャン行為。	3
ICMP ホスト照会 (ICMP Host Query)	1017	ICMP ホスト照会を示します。	3
UDP ホスト照会 (UDP Host Query)	1018	UDP ホスト照会を示します。	3
NMAP スキャン行為 (NMAP Reconnaissance)	1019	NMAP スキャン行為を示します。	3
TCP スキャン行為 (TCP Reconnaissance)	1020	ネットワークの TCP スキャン行為を示します。	3
UNIX スキャン行為	1021	UNIX ネットワークのスキャン行為。	3

表 82. スキャン行為イベント・カテゴリーの下位カテゴリーおよび重大度レベル (続き)

下位イベント・カテゴリー	カテゴリー ID	説明	重大度レベル (0 から 10 まで)
FTP スキャン行為 (FTP Reconnaissance)	1022	FTP スキャン行為を示します。	3

DoS

DoS カテゴリーには、サービスまたはホストに対するサービス妨害 (DoS) 攻撃に関連するイベントが含まれます。

以下の表で、DoS カテゴリーの下位イベント・カテゴリーおよび関連する重大度レベルについて説明します。

表 83. *DoS* イベント・カテゴリーの下位カテゴリーおよび重大度レベル

下位イベント・カテゴリー	カテゴリー ID	説明	重大度レベル (0 から 10 まで)
不明な DoS 攻撃 (Unknown DoS Attack)	2001	不明な DoS 攻撃を示します。	8
ICMP DoS	2002	ICMP DoS 攻撃を示します。	9
TCP DoS	2003	TCP DoS 攻撃を示します。	9
UDP DoS	2004	UDP DoS 攻撃を示します。	9
DNS サービス DoS (DNS Service DoS)	2005	DNS サービス DoS 攻撃を示します。	8
Web サービス DoS (Web Service DoS)	2006	Web サービス DoS 攻撃を示します。	8
メール・サービス DoS (Mail Service DoS)	2007	メール・サーバー DoS 攻撃を示します。	8
分散型 DoS	2008	分散型 DoS 攻撃を示します。	9
その他の DoS (Misc DoS)	2009	その他の DoS 攻撃を示します。	8
UNIX DoS	2010	UNIX DoS 攻撃を示します。	8
Windows DoS	2011	Windows DoS 攻撃を示します。	8
データベース DoS (Database DoS)	2012	データベース DoS 攻撃を示します。	8
FTP DoS	2013	FTP DoS 攻撃を示します。	8

表 *83. DoS* イベント・カテゴリーの下位カテゴリーおよび重大度レベル (続き)

下位イベント・カテゴリー	カテゴリー **ID**	説明	重大度レベル **(0** から **10** まで**)**
インフラストラクチャー DoS (Infrastructure DoS)	2014	インフラストラクチャーへの DoS 攻撃を示します。	8
Telnet DoS	2015	Telnet DoS 攻撃を示します。	8
ブルート・フォース・ログイン (Brute Force Login)	2016	無許可の方式によるシステムへのアクセスを示します。	8
高速 TCP DoS (High Rate TCP DoS)	2017	高速 TCP DoS 攻撃を示します。	8
高速 UDP DoS (High Rate UDP DoS)	2018	高速 UDP DoS 攻撃を示します。	8
高速 ICMP DoS (High Rate ICMP DoS)	2019	高速 ICMP DoS 攻撃を示します。	8
高速 DoS (High Rate DoS)	2020	高速 DoS 攻撃を示します。	8
中速 TCP DoS (Medium Rate TCP DoS)	2021	中速 TCP 攻撃を示します。	8
中速 UDP DoS (Medium Rate UDP DoS)	2022	中速 UDP 攻撃を示します。	8
中速 ICMP DoS (Medium Rate ICMP DoS)	2023	中速 ICMP 攻撃を示します。	8
中速 DoS (Medium Rate DoS)	2024	中速 DoS 攻撃を示します。	8
低速 TCP DoS (Low Rate TCP DoS)	2025	低速 TCP DoS 攻撃を示します。	8
低速 UDP DoS (Low Rate UDP DoS)	2026	低速 UDP DoS 攻撃を示します。	8
低速 ICMP DoS (Low Rate ICMP DoS)	2027	低速 ICMP DoS 攻撃を示します。	8
低速 DoS (Low Rate DoS)	2028	低速 DoS 攻撃を示します。	8
分散型高速 TCP DoS (Distributed High Rate TCP DoS)	2029	分散型高速 TCP DoS 攻撃を示します。	8

表 *83. DoS* イベント・カテゴリーの下位カテゴリーおよび重大度レベル *(*続き*)*

下位イベント・カテゴリー	カテゴリー **ID**	説明	重大度レベル **(0** から **10** まで**)**
分散型高速 UDP DoS (Distributed High Rate UDP DoS)	2030	分散型高速 UDP DoS 攻撃を示します。	8
分散型高速 ICMP DoS (Distributed High Rate ICMP DoS)	2031	分散型高速 ICMP DoS 攻撃を示します。	8
分散型高速 DoS (Distributed High Rate DoS)	2032	分散型高速 DoS 攻撃を示します。	8
分散型中速 TCP DoS (Distributed Medium Rate TCP DoS)	2033	分散型中速 TCP DoS 攻撃を示します。	8
分散型中速 UDP DoS (Distributed Medium Rate UDP DoS)	2034	分散型中速 UDP DoS 攻撃を示します。	8
分散型中速 ICMP DoS (Distributed Medium Rate ICMP DoS)	2035	分散型中速 ICMP DoS 攻撃を示します。	8
分散型中速 DoS (Distributed Medium Rate DoS)	2036	分散型中速 DoS 攻撃を示します。	8
分散型低速 TCP DoS (Distributed Low Rate TCP DoS)	2037	分散型低速 TCP DoS 攻撃を示します。	8
分散型低速 UDP DoS (Distributed Low Rate UDP DoS)	2038	分散型低速 UDP DoS 攻撃を示します。	8
分散型低速 ICMP DoS (Distributed Low Rate ICMP DoS)	2039	分散型低速 ICMP DoS 攻撃を示します。	8
分散型低速 DoS (Distributed Low Rate DoS)	2040	分散型低速 DoS 攻撃を示します。	8
高速 TCP スキャン (High Rate TCP Scan)	2041	高速 TCP スキャンを示します。	8
高速 UDP スキャン (High Rate UDP Scan)	2042	高速 UDP スキャンを示します。	8

表 *83. DoS* イベント・カテゴリーの下位カテゴリーおよび重大度レベル (続き)

下位イベント・カテゴリー	カテゴリー **ID**	説明	重大度レベル **(0** から **10** まで**)**
高速 ICMP スキャン (High Rate CMP Scan)	2043	高速 ICMP スキャンを示します。	8
高速スキャン	2044	高速スキャンを示します。	8
中速 TCP スキャン (Medium Rate TCP Scan)	2045	中速 TCP スキャンを示します。	8
中速 UDP スキャン (Medium Rate UDP Scan)	2046	中速 UDP スキャンを示します。	8
中速 ICMP スキャン (Medium Rate ICMP Scan)	2047	中速 ICMP スキャンを示します。	8
中速スキャン	2048	中速スキャンを示します。	8
低速 TCP スキャン (Low Rate TCP Scan)	2049	低速 TCP スキャンを示します。	8
低速 UDP スキャン (Low Rate UDP Scan)	2050	低速 UDP スキャンを示します。	8
低速 ICMP スキャン (Low Rate ICMP Scan)	2051	低速 ICMP スキャンを示します。	8
低速スキャン (Low Rate Scan)	2052	低速スキャンを示します。	8
VoIP DoS	2053	VoIP DoS 攻撃を示します。	8
フラッディング (Flood)	2054	フラッド攻撃を示します。	8
TCP フラッド (TCP Flood)	2055	TCP フラッド攻撃を示します。	8
UDP フラッド (UDP Flood)	2056	UDP フラッド攻撃を示します。	8
ICMP フラッド (ICMP Flood)	2057	ICMP フラッド攻撃を示します。	8
SYN フラッド (SYN Flood)	2058	SYN フラッド攻撃を示します。	8
URG フラッド (URG Flood)	2059	緊急 (URG) フラグをオンにしたフラッド攻撃を示します。	8

表 83. DoS イベント・カテゴリーの下位カテゴリーおよび重大度レベル (続き)

下位イベント・カテゴリー	カテゴリー ID	説明	重大度レベル (0 から 10 まで)
SYN URG フラッド (SYN URG Flood)	2060	緊急 (URG) フラグをオンにした SYN フラッド攻撃を示します。	8
SYN FIN フラッド (SYN FIN Flood)	2061	SYN FIN フラッド攻撃を示します。	8
SYN ACK フラッド (SYN ACK Flood)	2062	SYN ACK フラッド攻撃を示します。	8

認証

認証カテゴリーには、ネットワーク上のユーザーをモニターする認証、セッション、およびアクセス制御に関連したイベントが含まれます。

以下の表で、認証カテゴリーの下位イベント・カテゴリーおよび関連する重大度レベルについて説明します。

表 84. 認証イベント・カテゴリーの下位カテゴリーおよび重大度レベル

下位イベント・カテゴリー	カテゴリー ID	説明	重大度レベル (0 から 10 まで)
不明な認証 (Unknown Authentication)	3001	不明な認証を示します。	1
成功したホスト・ログイン (Host Login Succeeded)	3002	成功したホスト・ログインを示します。	1
失敗したホスト・ログイン (Host Login Failed)	3003	ホスト・ログインが失敗したことを示します。	3
成功したその他のログイン (Misc Login Succeeded)	3004	ログイン・シーケンスが成功したことを示します。	1
失敗したその他のログイン (Misc Login Failed)	3005	ログイン・シーケンスが失敗したことを示します。	3
失敗した特権のエスカレーション (Privilege Escalation Failed)	3006	特権のエスカレーションが失敗したことを示します。	3
成功した特権のエスカレーション (Privilege Escalation Succeeded)	3007	特権のエスカレーションが成功したことを示します。	1

表 84. 認証イベント・カテゴリーの下位カテゴリーおよび重大度レベル (続き)

下位イベント・カテゴリー	カテゴリー ID	説明	重大度レベル (0 から 10 まで)
成功したメール・サービスのログイン (Mail Service Login Succeeded)	3008	メール・サービスのログインが成功したことを示します。	1
失敗したメール・サービスのログイン (Mail Service Login Failed)	3009	メール・サービスのログインが失敗したことを示します。	3
ログインに失敗した認証サーバー (Auth Server Login Failed)	3010	認証サーバーのログインが失敗したことを示します。	3
ログインに成功した認証サーバー (Auth Server Login Succeeded)	3011	認証サーバーのログインが成功したことを示します。	1
ログインに成功した Web サービス (Web Service Login Succeeded)	3012	Web サービスのログインが成功したことを示します。	1
ログインに失敗した Web サービス (Web Service Login Failed)	3013	Web サービスのログインが失敗したことを示します。	3
成功した管理者ログイン (Admin Login Successful)	3014	管理者ログインが成功したことを示します。	1
失敗した管理者ログイン (Admin Login Failure)	3015	管理ログインが失敗したことを示します。	3
疑わしいユーザー名 (Suspicious Username)	3016	正しくないユーザー名をユーザーが使用して、ネットワークにアクセスしようとしたことを示します。	4
成功したデフォルトのユーザー名/パスワードによるログイン (Login with username/ password defaults successful)	3017	デフォルトのユーザー名およびパスワードを使用して、ユーザーがネットワークにアクセスしたことを示します。	4

表 84. 認証イベント・カテゴリーの下位カテゴリーおよび重大度レベル (続き)

下位イベント・カテゴリー	カテゴリー ID	説明	重大度レベル (0 から 10 まで)
失敗したデフォルトのユーザー名/パスワードによるログイン (Login with username/ password defaults failed)	3018	デフォルトのユーザー名およびパスワードを使用して、ユーザーがネットワークへのアクセスに失敗したことを示します。	4
成功した FTP ログイン (FTP Login Succeeded)	3019	FTP ログインが成功したことを示します。	1
失敗した FTP ログイン (FTP Login Failed)	3020	FTP ログインが失敗したことを示します。	3
成功した SSH ログイン (SSH Login Succeeded)	3021	SSH ログインが成功したことを示します。	1
失敗した SSH ログイン (SSH Login Failed)	3022	SSH ログインが失敗したことを示します。	2
割り当てられたユーザー権限 (User Right Assigned)	3023	ネットワーク・リソースへのユーザー・アクセス権限が正常に付与されたことを示します。	1
削除されたユーザー権限 (User Right Removed)	3024	ネットワーク・リソースへのユーザー・アクセスが正常に削除されたことを示します。	1
追加されたトラステッド・ドメイン (Trusted Domain Added)	3025	トラステッド・ドメインが正常にデプロイメントに追加されたことを示します。	1
削除されたトラステッド・ドメイン (Trusted Domain Removed)	3026	トラステッド・ドメインがデプロイメントから削除されたことを示します。	1
付与されたシステム・セキュリティー・アクセス権限 (System Security Access Granted)	3027	システム・セキュリティー・アクセス権限が正常に付与されたことを示します。	1

表 84. 認証イベント・カテゴリーの下位カテゴリーおよび重大度レベル (続き)

下位イベント・カテゴリー	カテゴリー ID	説明	重大度レベル (0 から 10 まで)
除去されたシステム・セキュリティー・アクセス権限 (System Security Access Removed)	3028	システム・セキュリティー・アクセス権限が正常に除去されたことを示します。	1
追加されたポリシー (Policy Added)	3029	ポリシーが正常に追加されたことを示します。	1
ポリシー変更 (Policy Change)	3030	ポリシーが正常に変更されたことを示します。	1
追加されたユーザー・アカウント (User Account Added)	3031	ユーザー・アカウントが正常に追加されたことを示します。	1
変更されたユーザー・アカウント (User Account Changed)	3032	既存のユーザー・アカウントへの変更を示します。	1
失敗したパスワード変更 (Password Change Failed)	3033	既存パスワードの変更の試行が失敗したことを示します。	3
成功したパスワード変更 (Password Change Succeeded)	3034	パスワード変更が成功したことを示します。	1
削除されたユーザー・アカウント (User Account Removed)	3035	ユーザー・アカウントが正常に削除されたことを示します。	1
追加されたグループ・メンバー (Group Member Added)	3036	グループ・メンバーが正常に追加されたことを示します。	1
削除されたグループ・メンバー (Group Member Removed)	3037	グループ・メンバーが削除されたことを示します。	1
追加されたグループ (Group Added)	3038	グループが正常に追加されたことを示します。	1
変更されたグループ (Group Changed)	3039	既存のグループへの変更を示します。	1
削除されたグループ (Group Removed)	3040	グループが削除されたことを示します。	1

表 84. 認証イベント・カテゴリーの下位カテゴリーおよび重大度レベル (続き)

下位イベント・カテゴリー	カテゴリー ID	説明	重大度レベル (0 から 10 まで)
追加されたコンピューター・アカウント (Computer Account Added)	3041	コンピューター・アカウントが正常に追加されたことを示します。	1
変更されたコンピューター・アカウント (Computer Account Changed)	3042	既存のコンピューター・アカウントへの変更を示します。	1
削除されたコンピューター・アカウント (Computer Account Removed)	3043	コンピューター・アカウントが正常に削除されたことを示します。	1
成功したリモート・アクセス・ログイン (Remote Access Login Succeeded)	3044	リモート・ログインを使用したネットワークへのアクセスが成功したことを示します。	1
失敗したリモート・アクセス・ログイン (Remote Access Login Failed)	3045	リモート・ログインを使用したネットワークへのアクセスが失敗したことを示します。	3
成功した一般認証 (General Authentication Successful)	3046	認証プロセスが成功したことを示します。	1
失敗した一般認証 (General Authentication Failed)	3047	認証プロセスが失敗したことを示します。	3
成功した Telnet ログイン (Telnet Login Succeeded)	3048	Telnet ログインが成功したことを示します。	1
失敗した Telnet ログイン (Telnet Login Failed)	3049	Telnet ログインが失敗したことを示します。	3
疑わしいパスワード (Suspicious Password)	3050	疑わしいパスワードをユーザーが使用してログインしようとしたことを示します。	4
成功した Samba ログイン (Samba Login Successful)	3051	ユーザーが Samba を使用して正常にログインしたことを示します。	1

表 84. 認証イベント・カテゴリーの下位カテゴリーおよび重大度レベル (続き)

下位イベント・カテゴリー	カテゴリー ID	説明	重大度レベル (0 から 10 まで)
失敗した Samba ログイン (Samba Login Failed)	3052	ユーザーが Samba を使用したログインに失敗したことを示します。	3
開かれた認証サーバーのセッション (Auth Server Session Opened)	3053	認証サーバーとの通信セッションが開始されたことを示します。	1
閉じられた認証サーバーのセッション (Auth Server Session Closed)	3054	認証サーバーとの通信セッションが閉じられたことを示します。	1
閉じられたファイアウォール・セッション (Firewall Session Closed)	3055	ファイアウォール・セッションが閉じられたことを示します。	1
ホストのログアウト (Host Logout)	3056	ホストが正常にログアウトしたことを示します。	1
その他のログアウト (Misc Logout)	3057	ユーザーが正常にログアウトしたことを示します。	1
認証サーバーのログアウト (Auth Server Logout)	3058	認証サーバーからログアウトするプロセスが成功したことを示します。	1
Web サービスのログアウト (Web Service Logout)	3059	Web サービスからログアウトするプロセスが成功したことを示します。	1
管理者のログアウト (Admin Logout)	3060	管理ユーザーが正常にログアウトしたことを示します。	1
FTP ログアウト (FTP Logout)	3061	FTP サービスからログアウトするプロセスが成功したことを示します。	1
SSH ログアウト (SSH Logout)	3062	SSH セッションからログアウトするプロセスが成功したことを示します。	1

表 84. 認証イベント・カテゴリーの下位カテゴリーおよび重大度レベル (続き)

下位イベント・カテゴリー	カテゴリー ID	説明	重大度レベル (0 から 10 まで)
リモート・アクセスのログアウト (Remote Access Logout)	3063	リモート・アクセスを使用してログアウトするプロセスが成功したことを示します。	1
Telnet ログアウト (Telnet Logout)	3064	Telnet セッションからログアウトするプロセスが成功したことを示します。	1
Samba ログアウト (Samba Logout)	3065	Samba からログアウトするプロセスが成功したことを示します。	1
開始された SSH セッション (SSH Session Started)	3066	ホスト上で SSH ログイン・セッションが開始されたことを示します。	1
終了した SSH セッション (SSH Session Finished)	3067	ホスト上での SSH ログイン・セッションの終了を示します。	1
開始された管理セッション (Admin Session Started)	3068	ホスト上でログイン・セッションが管理ユーザーまたは特権ユーザーにより開始されたことを示します。	1
終了した管理セッション (Admin Session Finished)	3069	ホスト上で管理者または特権ユーザーのログイン・セッションが終了したことを示します。	1
成功した VoIP ログイン (VoIP Login Succeeded)	3070	成功した VoIP サービス・ログインを示します。	1
失敗した VoIP ログイン (VoIP Login Failed)	3071	VoIP サービスへのアクセス試行が失敗したことを示します。	1
VoIP ログアウト (VoIP Logout)	3072	ユーザー・ログアウトを示します。	1
開始された VoIP セッション (VoIP Session Initiated)	3073	VoIP セッションの開始を示します。	1

表 84. 認証イベント・カテゴリーの下位カテゴリーおよび重大度レベル (続き)

下位イベント・カテゴリー	カテゴリー ID	説明	重大度レベル (0 から 10 まで)
終了した VoIP セッション (VoIP Session Terminated)	3074	VoIP セッションの終了を示します。	1
成功したデータベース・ログイン (Database Login Succeeded)	3075	成功したデータベース・ログインを示します。	1
失敗したデータベース・ログイン (Database Login Failure)	3076	データベース・ログインの試行が失敗したことを示します。	3
失敗した IKE 認証 (IKE Authentication Failed)	3077	失敗した Internet Key Exchange (IKE) 認証が検出されたことを示します。	3
成功した IKE 認証 (IKE Authentication Succeeded)	3078	成功した IKE 認証が検出されたことを示します。	1
開始された IKE セッション (IKE Session Started)	3079	IKE セッションが開始されたことを示します。	1
終了した IKE セッション (IKE Session Ended)	3080	IKE セッションが終了したことを示します。	1
IKE エラー (IKE Error)	3081	IKE エラー・メッセージを示します。	1
IKE 状況 (IKE Status)	3082	IKE 状況メッセージを示します。	1
開始された RADIUS セッション (RADIUS Session Started)	3083	RADIUS セッションが開始されたことを示します。	1
終了した RADIUS セッション (RADIUS Session Ended)	3084	RADIUS セッションが終了したことを示します。	1
拒否された RADIUS セッション (RADIUS Session Denied)	3085	RADIUS セッションが拒否されたことを示します。	1
RADIUS セッション状況 (RADIUS Session Status)	3086	RADIUS セッション状況メッセージを示します。	1
失敗した RADIUS 認証 (RADIUS Authentication Failed)	3087	RADIUS 認証障害を示します。	3

表 *84.* 認証イベント・カテゴリーの下位カテゴリーおよび重大度レベル (続き)

下位イベント・カテゴリー	カテゴリー **ID**	説明	重大度レベル **(0** から **10** まで**)**
成功した RADIUS 認証 (RADIUS Authentication Successful)	3088	RADIUS 認証が成功したことを示します。	1
開始された TACACS セッション (TACACS Session Started)	3089	TACACS セッションが開始されたことを示します。	1
終了した TACACS セッション (TACACS Session Ended)	3090	TACACS セッションが終了したことを示します。	1
拒否された TACACS セッション (TACACS Session Denied)	3091	TACACS セッションが拒否されたことを示します。	1
TACACS セッション状況 (TACACS Session Status)	3092	TACACS セッション状況メッセージを示します。	1
成功した TACACS 認証 (TACACS Authentication Successful)	3093	TACACS 認証が成功したことを示します。	1
失敗した TACACS 認証 (TACACS Authentication Failed)	3094	TACACS 認証障害を示します。	1
成功したホスト認証解除 (Deauthenticating Host Succeeded)	3095	ホストの認証解除が成功したことを示します。	1
失敗したホスト認証解除 (Deauthenticating Host Failed)	3096	ホストの認証解除が失敗したことを示します。	3
成功したステーション認証 (Station Authentication Succeeded)	3097	ステーション認証が成功したことを示します。	1
失敗したステーション認証 (Station Authentication Failed)	3098	ホストのステーション認証が失敗したことを示します。	3

表 84. 認証イベント・カテゴリーの下位カテゴリーおよび重大度レベル (続き)

下位イベント・カテゴリー	カテゴリー ID	説明	重大度レベル (0 から 10 まで)
成功したステーション関連付け (Station Association Succeeded)	3099	ステーション関連付けが成功したことを示します。	1
失敗したステーション関連付け (Station Association Failed)	3100	ステーション再関連付けが失敗したことを示します。	3
成功したステーション再関連付け (Station Reassociation Succeeded)	3101	ステーションの再関連付けが成功したことを示します。	1
失敗したステーション再関連付け (Station Reassociation Failed)	3102	ステーション再関連付けが失敗したことを示します。	3
成功したホスト関連付け解除 (Disassociating Host Succeeded)	3103	ホストの関連付け解除が成功したことを示します。	1
失敗したホスト関連付け解除 (Disassociating Host Failed)	3104	ホストの関連付け解除が失敗したことを示します。	3
SA エラー (SA Error)	3105	セキュリティー・アソシエーション (SA) エラー・メッセージを示します。	5
失敗した SA 作成 (SA Creation Failure)	3106	セキュリティー・アソシエーション (SA) 作成の失敗を示します。	3
確立された SA (SA Established)	3107	セキュリティー・アソシエーション (SA) 接続が確立されたことを示します。	1
拒否された SA (SA Rejected)	3108	セキュリティー・アソシエーション (SA) 接続が拒否されたことを示します。	3
SA の削除 (Deleting SA)	3109	セキュリティー・アソシエーション (SA) の削除を示します。	1

表 84. 認証イベント・カテゴリーの下位カテゴリーおよび重大度レベル (続き)

下位イベント・カテゴリー	カテゴリー ID	説明	重大度レベル (0 から 10 まで)
SA の作成 (Creating SA)	3110	セキュリティー・アソシエーション (SA) の作成を示します。	1
証明書の不一致 (Certificate Mismatch)	3111	証明書の不一致を示します。	3
資格情報の不一致 (Credentials Mismatch)	3112	資格情報の不一致を示します。	3
管理者ログイン試行 (Admin Login Attempt)	3113	管理者ログイン試行を示します。	2
ユーザー・ログイン試行 (User Login Attempt)	3114	ユーザー・ログイン試行を示します。	2
成功したユーザー・ログイン (User Login Successful)	3115	成功したユーザー・ログインを示します。	1
失敗したユーザー・ログイン (User Login Failure)	3116	失敗したユーザー・ログインを示します。	3
成功した SFTP ログイン (SFTP Login Succeeded)	3117	成功した SSH ファイル転送プロトコル (SFTP) ログインを示します。	1
SFTP ログイン失敗	3118	失敗した SSH ファイル転送プロトコル (SFTP) ログインを示します。	3
SFTP ログアウト (SFTP Logout)	3119	SSH ファイル転送プロトコル (SFTP) ログアウトを示します。	1
アイデンティティー付与	3120	アイデンティティーが付与されたことを示します。	1
アイデンティティー削除	3121	アイデンティティーが削除されたことを示します。	1
アイデンティティー取り消し	3122	アイデンティティーが取り消されたことを示します。	1
ポリシー削除	3123	ポリシーが削除されたことを示します。	1

表 84. 認証イベント・カテゴリーの下位カテゴリーおよび重大度レベル (続き)

下位イベント・カテゴリー	カテゴリー ID	説明	重大度レベル (0 から 10 まで)
ユーザー・アカウント・ロック	3124	ユーザー・アカウントがロックされたことを示します。	1
ユーザー・アカウント・アンロック	3125	ユーザー・アカウントがアンロックされたことを示します。	1
ユーザー・アカウント期限切れ	3126	ユーザー・アカウントが期限切れであることを示します。	1

アクセス

アクセス・カテゴリーには、ネットワーク・イベントをモニターするために使用される認証およびアクセス制御が含まれます。

以下の表で、アクセス・カテゴリーの下位イベント・カテゴリーおよび関連する重大度レベルについて説明します。

表 85. アクセス・イベント・カテゴリーの下位カテゴリーおよび重大度レベル

下位イベント・カテゴリー	カテゴリー ID	説明	重大度レベル (0 から 10 まで)
不明なネットワーク通信イベント (Unknown Network Communication Event)	4001	不明なネットワーク通信イベントを示します。	3
ファイアウォールの許可 (Firewall Permit)	4002	ファイアウォールへのアクセスが許可されたことを示します。	0
ファイアウォールの拒否 (Firewall Deny)	4003	ファイアウォールへのアクセスが拒否されたことを示します。	4
フロー・コンテキスト応答 (QRadar SIEM のみ)	4004	SIM 要求に応じて分類エンジンのイベントを示します。	5
その他のネットワーク通信イベント (Misc Network Communication Event)	4005	その他の通信イベントを示します。	3

表 *85.* アクセス・イベント・カテゴリーの下位カテゴリーおよび重大度レベル *(*続き*)*

下位イベント・カテゴリー	カテゴリー **ID**	説明	重大度レベル **(0** から **10** まで**)**
IPS の拒否 (IPS Deny)	4006	侵入防止システム (IPS) がトラフィックを拒否したことを示します。	4
開かれたファイアウォール・セッション (Firewall Session Opened)	4007	ファイアウォール・セッションが開かれたことを示します。	0
閉じられたファイアウォール・セッション (Firewall Session Closed)	4008	ファイアウォール・セッションが閉じられたことを示します。	0
成功した動的アドレス変換 (Dynamic Address Translation Successful)	4009	動的アドレス変換が成功したことを示します。	0
変換グループ検出なし	4010	変換グループが見つからないことを示します。	2
その他の権限 (Misc Authorization)	4011	アクセス権限がその他の認証サーバーに付与されたことを示します。	2
ACL の許可 (ACL Permit)	4012	アクセス制御リスト (ACL) がアクセスを許可したことを示します。	0
ACL の拒否 (ACL Deny)	4013	アクセス制御リスト (ACL) がアクセスを拒否したことを示します。	4
許可されたアクセス (Access Permitted)	4014	アクセスが許可されたことを示します。	0
拒否されたアクセス (Access Denied)	4015	アクセスが拒否されたことを示します。	4
開かれたセッション (Session Opened)	4016	セッションが開かれたことを示します。	1
閉じられたセッション (Session Closed)	4017	セッションが閉じられたことを示します。	1
リセットされたセッション (Session Reset)	4018	セッションがリセットされたことを示します。	3

表 85. アクセス・イベント・カテゴリーの下位カテゴリーおよび重大度レベル (続き)

下位イベント・カテゴリー	カテゴリー ID	説明	重大度レベル (0 から 10 まで)
終了したセッション (Session Terminated)	4019	セッションが許可されたことを示します。	4
拒否されたセッション (Session Denied)	4020	セッションが拒否されたことを示します。	5
進行中のセッション (Session in Progress)	4021	セッションが進行中であることを示します。	1
遅延したセッション (Session Delayed)	4022	セッションが遅延したことを示します。	3
キューに入れられたセッション (Session Queued)	4023	セッションがキューに入れられたことを示します。	1
セッション・インバウンド (Session Inbound)	4024	セッションがインバウンドであることを示します。	1
セッション・アウトバウンド (Session Outbound)	4025	セッションがアウトバウンドであることを示します。	1
無許可アクセスの試行 (Unauthorized Access Attempt)	4026	無許可アクセスの試行が検出されたことを示します。	6
許可されたその他のアプリケーション・アクション (Misc Application Action Allowed)	4027	アプリケーション・アクションが許可されたことを示します。	1
拒否されたその他のアプリケーション・アクション (Misc Application Action Denied)	4028	アプリケーション・アクションが拒否されたことを示します。	3
許可されたデータベース・アクション (Database Action Allowed)	4029	データベース・アクションが許可されたことを示します。	1
拒否されたデータベース・アクション (Database Action Denied)	4030	データベース・アクションが拒否されたことを示します。	3
許可された FTP アクション (FTP Action Allowed)	4031	FTP アクションが許可されたことを示します。	1

表 *85.* アクセス・イベント・カテゴリーの下位カテゴリーおよび重大度レベル (続き)

下位イベント・カテゴリー	カテゴリー **ID**	説明	重大度レベル **(0** から **10** まで**)**
拒否された FTP アクション (FTP Action Denied)	4032	FTP アクションが拒否されたことを示します。	3
キャッシュに入れられたオブジェクト (Object Cached)	4033	オブジェクトがキャッシュされたことを示します。	1
キャッシュに入れられていないオブジェクト (Object Not Cached)	4034	キャッシュに入れられていないオブジェクトを示します。	1
速度制限 (Rate Limiting)	4035	ネットワークがトラフィックの速度を制限することを示します。	4
速度制限なし (No Rate Limiting)	4036	ネットワークがトラフィックの速度を制限しないことを示します。	0
P11 アクセスの許可 (P11 Access Permitted)	4037	P11 アクセスが許可されていることを示します。	8
P11 アクセスの拒否 (P11 Access Denied)	4038	P11 アクセスが試行されて拒否されたことを示します。	8
IPS 許可	4039	IPS 許可を示します。	0

エクスプロイト (Exploit)

エクスプロイト・カテゴリーには、通信またはアクセスのエクスプロイトが発生したイベントが含まれます。

以下の表で、エクスプロイト・カテゴリーの下位イベント・カテゴリーおよび関連する重大度レベルについて説明します。

表 *86.* エクスプロイト・イベント・カテゴリーの下位カテゴリーおよび重大度レベル

下位イベント・カテゴリー	カテゴリー **ID**	説明	重大度レベル **(0** から **10** まで**)**
不明なエクスプロイト攻撃 (Unknown Exploit Attack)	5001	不明なエクスプロイト攻撃を示します。	9
バッファー・オーバーフロー (Buffer Overflow)	5002	バッファー・オーバーフローを示します。	9

表 86. エクスプロイト・イベント・カテゴリーの下位カテゴリーおよび重大度レベル (続き)

下位イベント・カテゴリー	カテゴリー ID	説明	重大度レベル (0 から 10 まで)
DNS エクスプロイト (DNS Exploit)	5003	DNS エクスプロイトを示します。	9
Telnet エクスプロイト (Telnet Exploit)	5004	Telnet エクスプロイトを示します。	9
Linux エクスプロイト (Linux Exploit)	5005	Linux エクスプロイトを示します。	9
UNIX エクスプロイト (UNIX Exploit)	5006	UNIX エクスプロイトを示します。	9
Windows エクスプロイト (Windows Exploit)	5007	Microsoft Windows エクスプロイトを示します。	9
メール・エクスプロイト (Mail Exploit)	5008	メール・サーバー・エクスプロイトを示します。	9
インフラストラクチャー・エクスプロイト (Infrastructure Exploit)	5009	インフラストラクチャー・エクスプロイトを示します。	9
その他のエクスプロイト (Misc Exploit)	5010	その他のエクスプロイトを示します。	9
Web エクスプロイト (Web Exploit)	5011	Web エクスプロイトを示します。	9
セッション・ハイジャック (Session Hijack)	5012	ネットワークのセッションが傍受されたことを示します。	9
アクティブなワーム (Worm Active)	5013	アクティブなワームを示します。	10
パスワードの予測/取得 (Password Guess/Retrieve)	5014	ユーザーがデータベースにパスワード情報へのアクセスを要求したことを示します。	9
FTP エクスプロイト (FTP Exploit)	5015	FTP エクスプロイトを示します。	9
RPC エクスプロイト (RPC Exploit)	5016	RPC エクスプロイトを示します。	9
SNMP エクスプロイト (SNMP Exploit)	5017	SNMP エクスプロイトを示します。	9
NOOP エクスプロイト (NOOP Exploit)	5018	NOOP エクスプロイトを示します。	9
Samba エクスプロイト (Samba Exploit)	5019	Samba エクスプロイトを示します。	9
SSH エクスプロイト (SSH Exploit)	5020	SSH エクスプロイトを示します。	9

表 86. エクスプロイト・イベント・カテゴリーの下位カテゴリーおよび重大度レベル (続き)

下位イベント・カテゴリー	カテゴリー ID	説明	重大度レベル (0 から 10 まで)
データベース・エクスプロイト (Database Exploit)	5021	データベース・エクスプロイトを示します。	9
ICMP エクスプロイト (ICMP Exploit)	5022	ICMP エクスプロイトを示します。	9
UDP エクスプロイト (UDP Exploit)	5023	UDP エクスプロイトを示します。	9
ブラウザー・エクスプロイト (Browser Exploit)	5024	ブラウザーへのエクスプロイトを示します。	9
DHCP エクスプロイト (DHCP Exploit)	5025	DHCP エクスプロイトを示します。	9
リモート・アクセス・エクスプロイト (Remote Access Exploit)	5026	リモート・アクセス・エクスプロイトを示します。	9
ActiveX エクスプロイト (ActiveX Exploit)	5027	ActiveX アプリケーションによるエクスプロイトを示します。	9
SQL インジェクション (SQL Injection)	5028	SQL インジェクションが発生したことを示します。	9
クロスサイト・スクリプティング (Cross-Site Scripting)	5029	クロスサイト・スクリプティングの脆弱性を示します。	9
フォーマット・ストリングの脆弱性 (Format String Vulnerability)	5030	フォーマット・ストリングの脆弱性を示します。	9
入力検証エクスプロイト (Input Validation Exploit)	5031	入力検証エクスプロイトの試行が検出されたことを示します。	9
リモート・コード実行 (Remote Code Execution)	5032	リモート・コード実行の試行が検出されたことを示します。	9
メモリー破壊 (Memory Corruption)	5033	メモリー破壊エクスプロイトが検出されたことを示します。	9
コマンド実行 (Command Execution)	5034	リモート・コマンド実行の試行が検出されたことを示します。	9

表 86. エクスプロイト・イベント・カテゴリーの下位カテゴリーおよび重大度レベル (続き)

下位イベント・カテゴリー	カテゴリー ID	説明	重大度レベル (0 から 10 まで)
コード注入	5035	コード注入が検出されたことを示します。	9
リプレイ・アタック	5036	リプレイ・アタックが検出されたことを示します。	9

マルウェア

悪意のあるソフトウェア (マルウェア) カテゴリーは、アプリケーションのエクスプロイトおよびバッファー・オーバーフローの試行に関連したイベントを示します。

以下の表で、マルウェア・カテゴリーの下位イベント・カテゴリーおよび関連する重大度レベルについて説明します。

表 87. マルウェア・イベント・カテゴリーの下位カテゴリーおよび重大度レベル

下位イベント・カテゴリー	カテゴリー ID	説明	重大度レベル (0 から 10 まで)
不明なマルウェア (Unknown Malware)	6001	不明なウィルスを示します。	4
検出されたバックドア (Backdoor Detected)	6002	システムのバックドアが検出されたことを示します。	9
悪意のあるメール添付 (Hostile Mail Attachment)	6003	悪意のあるメール添付を示します。	6
悪意のあるソフトウェア (Malicious Software)	6004	ウィルスを示します。	6
悪意のあるソフトウェアのダウンロード (Hostile Software Download)	6005	ネットワークへの、悪意のあるソフトウェアのダウンロードを示します。	6
検出されたウィルス (Virus Detected)	6006	ウィルスが検出されたことを示します。	8
その他のマルウェア (Misc Malware)	6007	その他の悪意のあるソフトウェアを示します。	4
検出されたトロイの木馬 (Trojan Detected)	6008	トロイの木馬が検出されたことを示します。	7
検出されたスパイウェア (Spyware Detected)	6009	スパイウェアがシステムで検出されたことを示します。	6

表 87. マルウェア・イベント・カテゴリーの下位カテゴリーおよび重大度レベル (続き)

下位イベント・カテゴリー	カテゴリー ID	説明	重大度レベル (0 から 10 まで)
コンテンツ・スキャン (Content Scan)	6010	コンテンツ・スキャンの試行が検出されたことを示します。	3
失敗したコンテンツ・スキャン (Content Scan Failed)	6011	コンテンツのスキャンが失敗したことを示します。	8
成功したコンテンツ・スキャン (Content Scan Successful)	6012	コンテンツのスキャンが成功したことを示します。	3
進行中のコンテンツ・スキャン (Content Scan in Progress)	6013	コンテンツのスキャンが進行中であることを示します。	3
キーロガー (Keylogger)	6014	キーロガーが検出されたことを示します。	7
検出されたアドウェア (Adware Detected)	6015	アドウェアが検出されたことを示します。	4
成功した検疫 (Quarantine Successful)	6016	検疫アクションが正常に完了したことを示します。	3
失敗した検疫 (Quarantine Failed)	6017	検疫アクションが失敗したことを示します。	8
マルウェア感染	6018	マルウェア感染が検出されたことを示します。	10
削除成功	6019	削除が正常に実行されたことを示します。	3
削除失敗	6020	削除が失敗したことを示します。	8

疑わしいアクティビティー

疑わしいアクティビティー・カテゴリーには、ウィルス、トロイの木馬、バックドア攻撃などの悪意のあるソフトウェアに関連するイベントが含まれます。

以下の表で、疑わしいアクティビティー・カテゴリーの下位イベント・カテゴリーとそれに関連する重大度レベルについて説明します。

表 *88.* 疑わしいアクティビティー・カテゴリーの下位イベント・カテゴリーと重大度レベル

下位イベント・カテゴリー	カテゴリー **ID**	説明	重大度レベル **(0** から **10** まで**)**
不明な疑わしいイベント (Unknown Suspicious Event)	7001	不明な疑わしいイベントを示します。	3
検出された疑わしいパターン (Suspicious Pattern Detected)	7002	疑わしいパターンが検出されたことを示します。	3
ファイアウォールによって変更されたコンテンツ (Content Modified By Firewall)	7003	コンテンツがファイアウォールによって変更されたことを示します。	3
無効なコマンドまたはデータ (Invalid Command or Data)	7004	無効なコマンドまたはデータを示します。	3
疑わしいパケット (Suspicious Packet)	7005	疑わしいパケットを示します。	3
疑わしいアクティビティー	7006	疑わしいアクティビティーを示します。	3
疑わしいファイル名 (Suspicious File Name)	7007	疑わしいファイル名を示します。	3
疑わしいポート・アクティビティー (Suspicious Port Activity)	7008	疑わしいポート・アクティビティーを示します。	3
疑わしいルーティング (Suspicious Routing)	7009	疑わしいルーティングを示します。	3
潜在的な Web 脆弱性 (Potential Web Vulnerability)	7010	潜在的な Web 脆弱性を示します。	3
不明な回避イベント (Unknown Evasion Event)	7011	不明な回避イベントを示します。	5
IP スプーフ (IP Spoof)	7012	IP スプーフを示します。	5
IP フラグメント (IP Fragmentation)	7013	IP フラグメントを示します。	3
オーバーラップしている IP フラグメント (Overlapping IP Fragments)	7014	オーバーラップしている IP フラグメントを示します。	5
IDS 回避 (IDS Evasion)	7015	IDS 回避を示します。	5

表 88. 疑わしいアクティビティー・カテゴリーの下位イベント・カテゴリーと重大度レベル (続き)

下位イベント・カテゴリー	カテゴリー ID	説明	重大度レベル (0 から 10 まで)
DNS プロトコル・アノマリ (DNS Protocol Anomaly)	7016	DNS プロトコル・アノマリを示します。	3
FTP プロトコル・アノマリ (FTP Protocol Anomaly)	7017	FTP プロトコル・アノマリを示します。	3
メール・プロトコル・アノマリ (Mail Protocol Anomaly)	7018	メール・プロトコル・アノマリを示します。	3
ルーティング・プロトコル・アノマリ (Routing Protocol Anomaly)	7019	ルーティング・プロトコル・アノマリを示します。	3
Web プロトコル・アノマリ (Web Protocol Anomaly)	7020	Web プロトコル・アノマリを示します。	3
SQL プロトコル・アノマリ (SQL Protocol Anomaly)	7021	SQL プロトコル・アノマリを示します。	3
検出された実行可能コード (Executable Code Detected)	7022	実行可能コードが検出されたことを示します。	5
その他の疑わしいイベント (Misc Suspicious Event)	7023	その他の疑わしいイベントを示します。	3
情報漏えい (Information Leak)	7024	情報漏えいを示します。	1
潜在的なメール脆弱性 (Potential Mail Vulnerability)	7025	メール・サーバーの潜在的な脆弱性を示します。	4
潜在的なバージョン脆弱性 (Potential Version Vulnerability)	7026	IBM Security QRadar バージョンの潜在的な脆弱性を示します。	4
潜在的な FTP 脆弱性 (Potential FTP Vulnerability)	7027	潜在的な FTP 脆弱性を示します。	4
潜在的な SSH 脆弱性 (Potential SSH Vulnerability)	7028	潜在的な SSH 脆弱性を示します。	4
潜在的な DNS 脆弱性 (Potential DNS Vulnerability)	7029	DNS サーバーの潜在的な脆弱性を示します。	4

表 *88.* 疑わしいアクティビティー・カテゴリーの下位イベント・カテゴリーと重大度レベル *(*続き*)*

下位イベント・カテゴリー	カテゴリー **ID**	説明	重大度レベル **(0** から **10** まで**)**
潜在的な SMB 脆弱性 (Potential SMB Vulnerability)	7030	潜在的な SMB (Samba) 脆弱性を示します。	4
潜在的なデータベース脆弱性 (Potential Database Vulnerability)	7031	データベースの潜在的な脆弱性を示します。	4
IP プロトコル・アノマリ (IP Protocol Anomaly)	7032	潜在的な IP プロトコル・アノマリを示します。	3
疑わしい IP アドレス (Suspicious IP Address)	7033	疑わしい IP アドレスが検出されたことを示します。	2
無効な IP プロトコルの使用法 (Invalid IP Protocol Usage)	7034	無効な IP プロトコルを示します。	2
無効なプロトコル (Invalid Protocol)	7035	無効なプロトコルを示します。	4
疑わしい Window イベント (Suspicious Window Events)	7036	デスクトップ上の画面での疑わしいイベントを示します。	2
疑わしい ICMP アクティビティー (Suspicious ICMP Activity)	7037	疑わしい ICMP アクティビティーを示します。	2
潜在的な NFS 脆弱性 (Potential NFS Vulnerability)	7038	潜在的なネットワーク・ファイル・システム (NFS) 脆弱性を示します。	4
潜在的な NNTP 脆弱性 (Potential NNTP Vulnerability)	7039	潜在的なネットワーク・ニュース転送プロトコル (NNTP) 脆弱性を示します。	4
潜在的な RPC 脆弱性 (Potential RPC Vulnerability)	7040	潜在的な RPC 脆弱性を示します。	4
潜在的な Telnet 脆弱性 (Potential Telnet Vulnerability)	7041	システム上の潜在的な Telnet 脆弱性を示します。	4
潜在的な SNMP 脆弱性 (Potential SNMP Vulnerability)	7042	潜在的な SNMP 脆弱性を示します。	4

表 88. 疑わしいアクティビティー・カテゴリーの下位イベント・カテゴリーと重大度レベル (続き)

下位イベント・カテゴリー	カテゴリー ID	説明	重大度レベル (0 から 10 まで)
正しくない TCP フラグの組み合わせ (Illegal CP Flag Combination)	7043	無効な TCP フラグの組み合わせが検出されたことを示します。	5
疑わしい TCP フラグの組み合わせ (Suspicious TCP Flag Combination)	7044	潜在的に無効な TCP フラグの組み合わせが検出されたことを示します。	4
正しくない ICMP プロトコルの使用法 (Illegal ICMP Protocol Usage)	7045	ICMP プロトコルの無効な使用が検出されたことを示します。	5
疑わしい ICMP プロトコルの使用法 (Suspicious ICMP Protocol Usage)	7046	ICMP プロトコルの潜在的に無効な使用が検出されたことを示します。	4
正しくない ICMP タイプ (Illegal ICMP Type)	7047	無効な ICMP タイプが検出されたことを示します。	5
正しくない ICMP コード (Illegal ICMP Code)	7048	無効な ICMP コードが検出されたことを示します。	5
疑わしい ICMP タイプ (Suspicious ICMP Type)	7049	潜在的に無効な ICMP タイプが検出されたことを示します。	4
疑わしい ICMP コード (Suspicious ICMP Code)	7050	潜在的に無効な ICMP コードが検出されたことを示します。	4
TCP ポート 0 (TCP port 0)	7051	送信元または宛先の予約ポート (0) を使用する TCP パケットを示します。	4
UDP ポート 0 (UDP port 0)	7052	送信元または宛先の予約ポート (0) を使用する UDP パケットを示します。	4
悪意のある IP (Hostile IP)	7053	既知の悪意のある IP アドレスの使用を示します。	4

表 *88.* 疑わしいアクティビティー・カテゴリーの下位イベント・カテゴリーと重大度レベル *(*続き*)*

下位イベント・カテゴリー	カテゴリー **ID**	説明	重大度レベル **(0** から **10** まで**)**
監視リスト IP (Watch list IP)	7054	IP アドレスの監視リストにある IP アドレスの使用を示します。	4
既知の違反者の IP (Known offender IP)	7055	既知の違反者の IP アドレスの使用を示します。	4
RFC 1918 (プライベート) IP (RFC 1918 (private) IP)	7056	プライベート IP アドレス範囲の IP アドレスの使用を示します。	4
潜在的な VoIP 脆弱性 (Potential VoIP Vulnerability)	7057	潜在的な VoIP 脆弱性を示します。	4
ブラックリスト・アドレス (Blacklist Address)	7058	IP アドレスがブラックリストにあることを示します。	8
監視リスト・アドレス (Watchlist Address)	7059	モニター対象の IP アドレスのリストに IP アドレスがあることを示します。	7
ダークネット・アドレス (Darknet Address)	7060	IP アドレスがダークネットに属していることを示します。	5
ボットネット・アドレス (Botnet Address)	7061	アドレスがボットネットに属していることを示します。	7
疑わしいアドレス (Suspicious Address)	7062	IP アドレスをモニターする必要があることを示します。	5
不正コンテンツ (Bad Content)	7063	不正コンテンツが検出されたことを示します。	7
無効な証明書 (Invalid Cert)	7064	無効な証明書が検出されたことを示します。	7
ユーザー・アクティビティー (User Activity)	7065	ユーザー・アクティビティーが検出されたことを示します。	7
疑わしいプロトコルの使用 (Suspicious Protocol Usage)	7066	疑わしいプロトコルの使用が検出されたことを示します。	5

表 *88.* 疑わしいアクティビティー・カテゴリーの下位イベント・カテゴリーと重大度レベル *(*続き*)*

下位イベント・カテゴリー	カテゴリー **ID**	説明	重大度レベル **(0** から **10** まで**)**
疑わしい BGP アクティビティー (Suspicious BGP Activity)	7067	疑わしいボーダー・ゲートウェイ・プロトコル (BGP) の使用が検出されたことを示します。	5
ルート・ポイズニング (Route Poisoning)	7068	ルートの破壊が検出されたことを示します。	5
ARP ポイズニング (ARP Poisoning)	7069	ARP キャッシュ・ポイズニングが検出されたことを示します。	5
検出された不良デバイス (Rogue Device Detected)	7070	不正なデバイスが検出されたことを示します。	5
政府機関アドレス	7071	政府機関アドレスが検出されたことを示します。	3

システム

システム・カテゴリーには、システムの変更、ソフトウェアのインストール、状況メッセージに関連するイベントが含まれます。

以下の表で、システム・カテゴリーの下位イベント・カテゴリーとそれに関連する重大度レベルについて説明します。

表 *89.* システム・カテゴリーの下位イベント・カテゴリーと重大度レベル

下位イベント・カテゴリー	カテゴリー **ID**	説明	重大度レベル **(0** から **10** まで**)**
不明なシステム・イベント (Unknown System Event)	8001	不明なシステム・イベントを示します。	1
システム・ブート (System Boot)	8002	システムの再始動を示します。	1
システム構成	8003	システム構成の変更を示します。	1
システム停止 (System Halt)	8004	システムが停止されたことを示します。	1
システム障害 (System Failure)	8005	サービス障害を示します。	6
システム状況 (System Status)	8006	すべての情報イベントを示します。	1

表 89. システム・カテゴリーの下位イベント・カテゴリーと重大度レベル (続き)

下位イベント・カテゴリー	カテゴリー ID	説明	重大度レベル (0 から 10 まで)
システム・エラー (System Error)	8007	システム・エラーを示します。	3
その他のシステム・イベント (Misc System Event)	8008	その他のシステム・イベントを示します。	1
サービス開始 (Service Started)	8009	システム・サービスが開始されたことを示します。	1
サービス停止 (Service Stopped)	8010	システム・サービスが停止したことを示します。	1
サービス障害 (Service Failure)	8011	サービス障害を示します。	6
成功したレジストリーの変更 (Successful Registry Modification)	8012	レジストリーの変更が成功したことを示します。	1
成功したホスト・ポリシーの変更 (Successful Host-Policy Modification)	8013	ホスト・ポリシーの変更が成功したことを示します。	1
成功したファイルの変更 (Successful File Modification)	8014	ファイルの変更が成功したことを示します。	1
成功したスタックの変更 (Successful Stack Modification)	8015	スタックの変更が成功したことを示します。	1
成功したアプリケーションの変更 (Successful Application Modification)	8016	アプリケーションの変更が成功したことを示します。	1
成功した構成の変更 (Successful Configuration Modification)	8017	構成の変更が成功したことを示します。	1
成功したサービスの変更 (Successful Service Modification)	8018	サービスの変更が成功したことを示します。	1
失敗したレジストリーの変更 (Failed Registry Modification)	8019	レジストリーの変更が失敗したことを示します。	1

表 89. システム・カテゴリーの下位イベント・カテゴリーと重大度レベル (続き)

下位イベント・カテゴリー	カテゴリー ID	説明	重大度レベル (0 から 10 まで)
失敗したホスト・ポリシーの変更 (Failed Host-Policy Modification)	8020	ホスト・ポリシーの変更が失敗したことを示します。	1
失敗したファイルの変更 (Failed File Modification)	8021	ファイルの変更が失敗したことを示します。	1
失敗したスタックの変更 (Failed Stack Modification)	8022	スタックの変更が失敗したことを示します。	1
失敗したアプリケーションの変更 (Failed Application Modification)	8023	アプリケーションの変更が失敗したことを示します。	1
失敗した構成の変更 (Failed Configuration Modification)	8024	構成の変更が失敗したことを示します。	1
失敗したサービスの変更 (Failed Service Modification)	8025	サービスの変更が失敗したことを示します。	1
レジストリーの追加 (Registry Addition)	8026	新しい項目がレジストリーに追加されたことを示します。	1
作成されたホスト・ポリシー (Host-Policy Create)	8027	新しい項目がレジストリーに追加されたことを示します。	1
作成されたファイル (File Created)	8028	新しいファイルがシステムに作成されたことを示します。	1
インストールされたアプリケーション (Application Installed)	8029	新しいアプリケーションがシステムにインストールされたことを示します。	1
インストールされたサービス (Service Installed)	8030	新しいサービスがシステムにインストールされたことを示します。	1
レジストリーの削除 (Registry Deletion)	8031	レジストリー項目が削除されたことを示します。	1
削除されたホスト・ポリシー (Host-Policy Deleted)	8032	ホスト・ポリシー項目が削除されたことを示します。	1
削除されたファイル (File Deleted)	8033	ファイルが削除されたことを示します。	1

表 89. システム・カテゴリーの下位イベント・カテゴリーと重大度レベル (続き)

下位イベント・カテゴリー	カテゴリー ID	説明	重大度レベル (0 から 10 まで)
アンインストールされたアプリケーション (Application Uninstalled)	8034	アプリケーションがアンインストールされたことを示します。	1
アンインストールされたサービス (Service Uninstalled)	8035	サービスがアンインストールされたことを示します。	1
システム情報 (System Informational)	8036	システム情報を示します。	3
システム処置の許可 (System Action Allow)	8037	システム上で試行された処置が許可されたことを示します。	3
システム処置の拒否 (System Action Deny)	8038	システム上で試行された処置が拒否されたことを示します。	4
クーロン (Cron)	8039	crontab メッセージを示します。	1
クーロン状況 (Cron Status)	8040	crontab 状況メッセージを示します。	1
失敗したクーロン	8041	crontab 失敗メッセージを示します。	4
成功したクーロン	8042	crontab 成功メッセージを示します。	1
デーモン	8043	デーモン・メッセージを示します。	1
デーモン状況	8044	デーモン状況メッセージを示します。	1
失敗したデーモン (Daemon Failed)	8045	デーモン失敗メッセージを示します。	4
成功したデーモン (Daemon Successful)	8046	デーモン成功メッセージを示します。	1
カーネル (Kernel)	8047	カーネル・メッセージを示します。	1
カーネル状況 (Kernel Status)	8048	カーネル状況メッセージを示します。	1
失敗したカーネル (Kernel Failed)	8049	カーネル失敗メッセージを示します。	
成功したカーネル (Kernel Successful)	8050	カーネル成功メッセージを示します。	1
認証	8051	認証メッセージを示します。	1
情報 (Information)	8052	情報メッセージを示します。	2

表 89. システム・カテゴリーの下位イベント・カテゴリーと重大度レベル (続き)

下位イベント・カテゴリー	カテゴリー ID	説明	重大度レベル (0 から 10 まで)
通知 (Notice)	8053	通知メッセージを示します。	3
警告 (Warning)	8054	警告メッセージを示します。	5
エラー (Error)	8055	エラー・メッセージを示します。	7
重要 (Critical)	8056	重要なメッセージを示します。	9
デバッグ (Debug)	8057	デバッグ・メッセージを示します。	1
メッセージ (Messages)	8058	汎用メッセージを示します。	1
特権アクセス (Privilege Access)	8059	特権アクセスが試行されたことを示します。	3
アラート (Alert)	8060	アラート・メッセージを示します。	9
緊急 (Emergency)	8061	緊急メッセージを示します。	9
SNMP 状況 (SNMP Status)	8062	SNMP 状況メッセージを示します。	1
FTP 状況 (FTP Status)	8063	FTP 状況メッセージを示します。	1
NTP 状況 (NTP Status)	8064	NTP 状況メッセージを示します。	1
アクセス・ポイント無線障害 (Access Point Radio Failure)	8065	アクセス・ポイント無線障害を示します。	3
暗号化プロトコル構成の不一致 (Encryption Protocol Configuration Mismatch)	8066	暗号化プロトコル構成の不一致を示します。	3
誤った構成のクライアント・デバイスまたは認証サーバー (Client Device or Authentication Server Misconfigured)	8067	クライアント・デバイスまたは認証サーバーが正しく構成されていないことを示します。	5
失敗したホット・スタンバイ有効化 (Hot Standby Enable Failed)	8068	ホット・スタンバイ有効化の失敗を示します。	5

表 89. システム・カテゴリーの下位イベント・カテゴリーと重大度レベル (続き)

下位イベント・カテゴリー	カテゴリー ID	説明	重大度レベル (0 から 10 まで)
失敗したホット・スタンバイ無効化 (Hot Standby Disable Failed)	8069	ホット・スタンバイ無効化の失敗を示します。	5
成功したホット・スタンバイ有効化 (Hot Standby Enabled Successfully)	8070	ホット・スタンバイが正常に有効化されたことを示します。	1
失われたホット・スタンバイ関連付け (Hot Standby Association Lost)	8071	ホット・スタンバイの関連付けが失われたことを示します。	5
失敗したメイン・モード開始 (MainMode Initiation Failure)	8072	失敗したメイン・モード開始を示します。	5
成功したメイン・モード開始 (MainMode Initiation Succeeded)	8073	メイン・モード開始が成功したことを示します。	1
メイン・モード状況 (MainMode Status)	8074	メイン・モード状況メッセージが報告されたことを示します。	1
失敗したクイック・モード開始 (QuickMode Initiation Failure)	8075	クイック・モード開始が失敗したことを示します。	5
成功したクイック・モード開始 (Quickmode Initiation Succeeded)	8076	クイック・モード開始が成功したことを示します。	1
クイック・モード状況 (Quickmode Status)	8077	クイック・モード状況メッセージが報告されたことを示します。	1
無効なライセンス (Invalid License)	8078	無効なライセンスを示します。	3
有効期限が切れたライセンス (License Expired)	8079	有効期限が切れたライセンスを示します。	3
適用された新規ライセンス (New License Applied)	8080	適用された新規ライセンスを示します。	1
ライセンス・エラー (License Error)	8081	ライセンス・エラーを示します。	5

表 89. システム・カテゴリーの下位イベント・カテゴリーと重大度レベル (続き)

下位イベント・カテゴリー	カテゴリー ID	説明	重大度レベル (0 から 10 まで)
ライセンスの状況	8082	ライセンス状況メッセージを示します。	1
構成エラー (Configuration Error)	8083	構成エラーが検出されたことを示します。	5
サービスの中断 (Service Disruption)	8084	サービスの中断が検出されたことを示します。	5
EPS または FPM 割り振りの超過	8085	EPS または FPM のライセンス・プール割り振りが超過したことを示します。	3
パフォーマンス状況 (Performance Status)	8086	パフォーマンス状況が報告されたことを示します。	1
パフォーマンス低下 (Performance Degradation)	8087	パフォーマンスが低下していることを示します。	4
誤った構成 (Misconfiguration)	8088	正しくない構成が検出されたことを示します。	5

ポリシー

ポリシー・カテゴリーは、ネットワーク・ポリシーの管理とネットワーク・リソースのポリシー違反のモニターに関連したイベントを示します。

以下の表で、ポリシー・カテゴリーの下位イベント・カテゴリーおよび重大度レベルについて説明します。

表 90. ポリシー・カテゴリーの下位カテゴリーおよび重大度レベル

下位イベント・カテゴリー	カテゴリー ID	説明	重大度レベル (0 から 10 まで)
不明なポリシー違反 (Unknown Policy Violation)	9001	不明なポリシー違反を示します。	2
Web ポリシー違反 (Web Policy Violation)	9002	Web ポリシー違反を示します。	2
リモート・アクセス・ポリシー違反 (Remote Access Policy Violation)	9003	リモート・アクセス・ポリシー違反を示します。	2

表 *90.* ポリシー・カテゴリーの下位カテゴリーおよび重大度レベル (続き)

下位イベント・カテゴリー	カテゴリー **ID**	説明	重大度レベル **(0** から **10** まで**)**
IRC/IM ポリシー違反 (IRC/IM Policy Violation)	9004	インスタント・メッセンジャーのポリシー違反を示します。	2
P2P ポリシー違反 (P2P Policy Violation)	9005	対等通信 (P2P) ポリシー違反を示します。	2
IP アクセス・ポリシー違反 (IP Access Policy Violation)	9006	IP アクセス・ポリシー違反を示します。	2
アプリケーション・ポリシー違反 (Application Policy Violation)	9007	アプリケーション・ポリシー違反を示します。	2
データベース・ポリシー違反 (Database Policy Violation)	9008	データベース・ポリシー違反を示します。	2
ネットワークしきい値ポリシー違反 (Network Threshold Policy Violation)	9009	ネットワークしきい値ポリシー違反を示します。	2
ポルノ・ポリシー違反 (Porn Policy Violation)	9010	ポルノ・ポリシー違反を示します。	2
ゲーム・ポリシー違反 (Games Policy Violation)	9011	ゲーム・ポリシー違反を示します。	2
その他のポリシー違反 (Misc Policy Violation)	9012	その他のポリシー違反を示します。	2
コンプライアンス・ポリシー違反 (Compliance Policy Violation)	9013	コンプライアンス・ポリシー違反を示します。	2
メール・ポリシー違反 (Mail Policy Violation)	9014	メール・ポリシー違反を示します。	2
IRC ポリシー違反 (IRC Policy Violation)	9015	IRC ポリシー違反を示します。	2
IM ポリシー違反 (IM Policy Violation)	9016	インスタント・メッセージ (IM) アクティビティーに関連したポリシー違反を示します。	2

表 *90.* ポリシー・カテゴリーの下位カテゴリーおよび重大度レベル (続き)

下位イベント・カテゴリー	カテゴリー **ID**	説明	重大度レベル **(0** から **10** まで**)**
VoIP ポリシー違反 (VoIP Policy Violation)	9017	VoIP ポリシー違反を示します。	2
成功 (Succeeded)	9018	ポリシー成功メッセージを示します。	1
失敗 (Failed)	9019	ポリシー失敗メッセージを示します。	4
データ損失防止ポリシー違反行為	9020	データ損失防止ポリシー違反行為を示します。	2
監査リスト・オブジェクト	9021	監視リスト・オブジェクトを示します。	2
Web ポリシー許可	9022	新しい Web ポリシー許可を示します。	1

不明

不明カテゴリーには、解析されていないためにカテゴリー化できないイベントが含まれます。

以下の表で、不明カテゴリーの下位イベント・カテゴリーとそれに関連する重大度レベルについて説明します。

表 *91.* 不明カテゴリーの下位イベント・カテゴリーと重大度レベル

下位イベント・カテゴリー	カテゴリー **ID**	説明	重大度レベル **(0** から **10** まで**)**
不明	10001	不明なイベントを示します。	3
不明な Snort イベント (Unknown Snort Event)	10002	不明な Snort イベントを示します。	3
不明な Dragon イベント (Unknown Dragon Event)	10003	不明な Dragon イベントを示します。	3
不明な Pix ファイアウォール・イベント (Unknown Pix Firewall Event)	10004	不明な Cisco Private Internet Exchange (PIX) ファイアウォール イベントを示します。	3
不明な Tipping Point イベント (Unknown Tipping Point Event)	10005	不明な HP TippingPoint イベントを示します。	3

表 91. 不明カテゴリーの下位イベント・カテゴリーと重大度レベル (続き)

下位イベント・カテゴリー	カテゴリー ID	説明	重大度レベル (0 から 10 まで)
不明な Windows 認証サーバー・イベント	10006	不明な Windows 認証サーバー イベントを示します。	3
不明な Nortel イベント (Unknown Nortel Event)	10007	不明な Nortel イベントを示します。	3
保管 (Stored)	10009	不明な保管イベントを示します。	3
振る舞い	11001	不明な振る舞いイベントを示します。	3
しきい値 (Threshold)	11002	不明なしきい値イベントを示します。	3
アノマリ (Anomaly)	11003	不明なアノマリ・イベントを示します。	3

CRE

カスタム・ルール・イベント (CRE) カテゴリーには、カスタム・オフェンス、フロー、またはイベントのルールから生成されるイベントが含まれます。

以下の表で、CRE カテゴリーの下位イベント・カテゴリーおよび関連する重大度レベルについて説明します。

表 92. CRE カテゴリーの下位カテゴリーおよび重大度レベル

下位イベント・カテゴリー	カテゴリー ID	説明	重大度レベル (0 から 10 まで)
不明な CRE イベント (Unknown CRE Event)	12001	不明なカスタム・ルール・エンジン・イベントを示します。	5
単一のイベントルールの一致 (Single Event Rule Match)	12002	単一のイベントルールの一致を示します。	5
イベント順序ルールの一致 (Event Sequence Rule Match)	12003	イベント順序ルールの一致を示します。	5
オフェンスをまたぐイベント順序ルールの一致 (Cross-Offense Event Sequence Rule Match)	12004	オフェンスをまたぐイベント順序ルールの一致を示します。	5
オフェンスルールの一致 (Offense Rule Match)	12005	オフェンスルールの一致を示します。	5

潜在的エクスプロイト

潜在的エクスプロイト・カテゴリーは、潜在的なアプリケーションのエクスプロイトおよびバッファー・オーバーフローの試行に関連したイベントを示します。

以下の表で、潜在的エクスプロイト・カテゴリーの下位イベント・カテゴリーおよび関連する重大度レベルについて説明します。

表 *93.* 潜在的エクスプロイト・カテゴリーの下位カテゴリーおよび重大度レベル

下位イベント・カテゴリー	カテゴリー **ID**	説明	重大度レベル **(0** から **10** まで**)**
不明な潜在的エクスプロイト攻撃 (Unknown Potential Exploit Attack)	13001	潜在的エクスプロイト攻撃が検出されたことを示します。	7
潜在的なバッファー・オーバーフロー (Potential Buffer Overflow)	13002	潜在的なバッファー・オーバーフローが検出されたことを示します。	7
潜在的なDNS エクスプロイト (Potential DNS Exploit)	13003	DNS サーバーによる潜在的エクスプロイト攻撃が検出されたことを示します。	7
潜在的な Telnet エクスプロイト (Potential Telnet Exploit)	13004	Telnet による潜在的エクスプロイト攻撃が検出されたことを示します。	7
潜在的な Linux エクスプロイト (Potential Linux Exploit)	13005	Linux による潜在的エクスプロイト攻撃が検出されたことを示します。	7
潜在的な UNIX エクスプロイト	13006	UNIX による潜在的エクスプロイト攻撃が検出されたことを示します。	7
潜在的な Windows エクスプロイト (Potential Windows Exploit)	13007	Windows による潜在的エクスプロイト攻撃が検出されたことを示します。	7
潜在的なメール・エクスプロイト	13008	メールによる潜在的エクスプロイト攻撃が検出されたことを示します。	7

表 93. 潜在的エクスプロイト・カテゴリーの下位カテゴリーおよび重大度レベル (続き)

下位イベント・カテゴリー	カテゴリー ID	説明	重大度レベル (0 から 10 まで)
潜在的なインフラストラクチャー・エクスプロイト (Potential Infrastructure Exploit)	13009	システム・インフラストラクチャーへの潜在的エクスプロイト攻撃が検出されたことを示します。	7
潜在的なその他のエクスプロイト (Potential Misc Exploit)	13010	潜在的エクスプロイト攻撃が検出されたことを示します。	7
潜在的な Web エクスプロイト (Potential Web Exploit)	13011	Web による潜在的エクスプロイト攻撃が検出されたことを示します。	7
潜在的なボットネット接続 (Potential Botnet Connection)	13012	ボットネットを使用した潜在的エクスプロイト攻撃が検出されたことを示します。	6
潜在的なワーム・アクティビティー (Potential Worm Activity)	13013	ワーム・アクティビティーを使用した潜在的攻撃が検出されたことを示します。	6

フロー

フロー・カテゴリーには、フロー・アクションに関するイベントが含まれます。

以下の表で、フロー・カテゴリーの下位イベント・カテゴリーおよび関連する重大度レベルについて説明します。

表 94. フロー・カテゴリーの下位カテゴリーおよび重大度レベル

下位イベント・カテゴリー	カテゴリー ID	説明	重大度レベル (0 から 10 まで)
単一方向フロー	14001	イベントの単一方向フローを示します。	5
少数の単一方向フロー	14002	イベントの少数の単一方向フローを示します。	5
中程度の数の単一方向フロー	14003	イベントの中程度の数の単一方向フローを示します。	5
多数の単一方向フロー	14004	イベントの多数の単一方向フローを示します。	5
単一方向 TCP フロー	14005	単一方向 TCP フローを示します。	5
少数の単一方向 TCP フロー	14006	少数の単一方向 TCP フローを示します。	5

表 94. フロー・カテゴリーの下位カテゴリーおよび重大度レベル (続き)

下位イベント・カテゴリー	カテゴリー ID	説明	重大度レベル (0 から 10 まで)
中程度の数の単一方向 TCP フロー	14007	中程度の数の単一方向 TCP フローを示します。	5
多数の単一方向 TCP フロー	14008	多数の単一方向 TCP フローを示します。	5
単一方向 ICMP フロー	14009	単一方向 ICMP フローを示します。	5
少数の単一方向 ICMP フロー	14010	少数の単一方向 ICMP フローを示します。	5
中程度の数の単一方向 ICMP フロー	14011	中程度の数の単一方向 ICMP フローを示します。	5
多数の単一方向 ICMP フロー	14012	多数の単一方向 ICMP フローを示します。	5
疑わしい ICMP フロー	14013	疑わしい ICMP フローを示します。	5
疑わしい UDP フロー	14014	疑わしい UDP フローを示します。	5
疑わしい TCP フロー	14015	疑わしい TCP フローを示します。	5
疑わしいフロー	14016	疑わしいフローを示します。	5
空のパケット・フロー	14017	空のパケット・フローを示します。	5
少数の空のパケット・フロー	14018	少数の空のパケット・フローを示します。	5
中程度の数の空のパケット・フロー	14019	中程度の数の空のパケット・フローを示します。	5
多数の空のパケット・フロー	14020	多数の空のパケット・フローを示します。	5
大規模ペイロード・フロー	14021	フローの大規模ペイロードを示します。	5
少数の大規模ペイロード・フロー	14022	少数の大規模ペイロード・フローを示します。	5
中程度の数の大規模ペイロード・フロー	14023	中程度の数の大規模ペイロード・フローを示します。	5
多数の大規模ペイロード・フロー	14024	多数の大規模ペイロード・フローを示します。	5
1 人の攻撃者から多数のターゲットへのフロー	14025	1 人の攻撃者が多数のフローをターゲットにしていることを示します。	5
多数の攻撃者から 1 つのターゲットへのフロー	14026	多数の攻撃者が 1 つのフローをターゲットにしていることを示します。	5
不明なフロー	14027	不明なフローを示します。	5

表 94. フロー・カテゴリーの下位カテゴリーおよび重大度レベル (続き)

下位イベント・カテゴリー	カテゴリー ID	説明	重大度レベル (0 から 10 まで)
Netflow レコード	14028	Netflow レコードを示します。	5
QFlow レコード	14029	QFlow レコードを示します。	5
SFlow レコード	14030	SFlow レコードを示します。	5
Packeteer レコード	14031	Packeteer レコードを示します。	5
その他のフロー	14032	その他のフローを示します。	5
大容量データ転送	14033	データの大規模な転送を示します。	5
大容量のアウトバウンドのデータ転送	14034	アウトバウンド・データの大規模な転送を示します。	5
VoIP フロー	14035	VoIP フローを示します。	5

ユーザー定義

ユーザー定義カテゴリーには、ユーザー定義オブジェクトに関連するイベントが含まれます。

以下の表で、ユーザー定義カテゴリーの下位イベント・カテゴリーとそれに関連する重大度レベルについて説明します。

表 95. ユーザー定義カテゴリーの下位イベント・カテゴリーと重大度レベル

下位イベント・カテゴリー	カテゴリー ID	説明	重大度レベル (0 から 10 まで)
カスタムの監視機能 (低) (Custom Sentry Low)	15001	重大度が低いカスタム・アノマリ・イベントを示します。	3
カスタムの監視機能 (中) (Custom Sentry Medium)	15002	重大度が中程度のカスタム・アノマリ・イベントを示します。	5
カスタムの監視機能 (高) (Custom Sentry High)	15003	重大度が高いカスタム・アノマリ・イベントを示します。	7
カスタムの監視機能 1 (Custom Sentry 1)	15004	重大度レベルが 1 のカスタム・アノマリ・イベントを示します。	1

表 *95.* ユーザー定義カテゴリーの下位イベント・カテゴリーと重大度レベル (続き)

下位イベント・カテゴリー	カテゴリー **ID**	説明	重大度レベル **(0** から **10** まで**)**
カスタムの監視機能 2 (Custom Sentry 2)	15005	重大度レベルが 2 のカスタム・アノマリ・イベントを示します。	2
カスタムの監視機能 3 (Custom Sentry 3)	15006	重大度レベルが 3 のカスタム・アノマリ・イベントを示します。	3
カスタムの監視機能 4 (Custom Sentry 4)	15007	重大度レベルが 4 のカスタム・アノマリ・イベントを示します。	4
カスタムの監視機能 5 (Custom Sentry 5)	15008	重大度レベルが 5 のカスタム・アノマリ・イベントを示します。	5
カスタムの監視機能 6 (Custom Sentry 6)	15009	重大度レベルが 6 のカスタム・アノマリ・イベントを示します。	6
カスタムの監視機能 7 (Custom Sentry 7)	15010	重大度レベルが 7 のカスタム・アノマリ・イベントを示します。	7
カスタムの監視機能 8 (Custom Sentry 8)	15011	重大度レベルが 8 のカスタム・アノマリ・イベントを示します。	8
カスタムの監視機能 9 (Custom Sentry 9)	15012	重大度レベルが 9 のカスタム・アノマリ・イベントを示します。	9
カスタム・ポリシー (低) (Custom Policy Low)	15013	重大度レベルが低いカスタム・ポリシー・イベントを示します。	3
カスタム・ポリシー (中) (Custom Policy Medium)	15014	重大度レベルが中程度のカスタム・ポリシー・イベントを示します。	5
カスタム・ポリシー (高) (Custom Policy High)	15015	重大度レベルが高いカスタム・ポリシー・イベントを示します。	7

表 95. ユーザー定義カテゴリーの下位イベント・カテゴリーと重大度レベル (続き)

下位イベント・カテゴリー	カテゴリー ID	説明	重大度レベル (0 から 10 まで)
カスタム・ポリシー 1 (Custom Policy 1)	15016	重大度レベルが 1 のカスタム・ポリシー・イベントを示します。	1
カスタム・ポリシー 2 (Custom Policy 2)	15017	重大度レベルが 2 のカスタム・ポリシー・イベントを示します。	2
カスタム・ポリシー 3 (Custom Policy 3)	15018	重大度レベルが 3 のカスタム・ポリシー・イベントを示します。	3
カスタム・ポリシー 4 (Custom Policy 4)	15019	重大度レベルが 4 のカスタム・ポリシー・イベントを示します。	4
カスタム・ポリシー 5 (Custom Policy 5)	15020	重大度レベルが 5 のカスタム・ポリシー・イベントを示します。	5
カスタム・ポリシー 6 (Custom Policy 6)	15021	重大度レベルが 6 のカスタム・ポリシー・イベントを示します。	6
カスタム・ポリシー 7 (Custom Policy 7)	15022	重大度レベルが 7 のカスタム・ポリシー・イベントを示します。	7
カスタム・ポリシー 8 (Custom Policy 8)	15023	重大度レベルが 8 のカスタム・ポリシー・イベントを示します。	8
カスタム・ポリシー 9 (Custom Policy 9)	15024	重大度レベルが 9 のカスタム・ポリシー・イベントを示します。	9
カスタム・ユーザー (低) (Custom User Low)	15025	重大度レベルが低いカスタム・ユーザー・イベントを示します。	3
カスタム・ユーザー (中) (Custom User Medium)	15026	重大度レベルが中程度のカスタム・ユーザー・イベントを示します。	5

表 95. ユーザー定義カテゴリーの下位イベント・カテゴリーと重大度レベル (続き)

下位イベント・カテゴリー	カテゴリー ID	説明	重大度レベル (0 から 10 まで)
カスタム・ユーザー (高) (Custom User High)	15027	重大度レベルが高いカスタム・ユーザー・イベントを示します。	7
カスタム・ユーザー 1 (Custom User 1)	15028	重大度レベルが 1 のカスタム・ユーザー・イベントを示します。	1
カスタム・ユーザー 2 (Custom User 2)	15029	重大度レベルが 2 のカスタム・ユーザー・イベントを示します。	2
カスタム・ユーザー 3 (Custom User 3)	15030	重大度レベルが 3 のカスタム・ユーザー・イベントを示します。	3
カスタム・ユーザー 4 (Custom User 4)	15031	重大度レベルが 4 のカスタム・ユーザー・イベントを示します。	4
カスタム・ユーザー 5 (Custom User 5)	15032	重大度レベルが 5 のカスタム・ユーザー・イベントを示します。	5
カスタム・ユーザー 6 (Custom User 6)	15033	重大度レベルが 6 のカスタム・ユーザー・イベントを示します。	6
カスタム・ユーザー 7 (Custom User 7)	15034	重大度レベルが 7 のカスタム・ユーザー・イベントを示します。	7
カスタム・ユーザー 8 (Custom User 8)	15035	重大度レベルが 8 のカスタム・ユーザー・イベントを示します。	8
カスタム・ユーザー 9 (Custom User 9)	15036	重大度レベルが 9 のカスタム・ユーザー・イベントを示します。	9

SIM 監査

SIM 監査カテゴリーには、IBM Security QRadar コンソールと管理機能でのユーザー操作に関連するイベントが含まれます。

以下の表で、SIM 監査カテゴリーの下位イベント・カテゴリーとそれに関連する重大度レベルについて説明します。

表 *96. SIM* 監査カテゴリーの下位イベント・カテゴリーと重大度レベル

下位イベント・カテゴリー	カテゴリー **ID**	説明	重大度レベル **(0** から **10** まで**)**
SIM ユーザー認証 (SIM User Authentication)	16001	コンソールでのユーザーのログインまたはログアウトを示します。	5
SIM 構成変更 (SIM Configuration Change)	16002	ユーザーが SIM の構成またはデプロイメント環境を変更したことを示します。	3
SIM ユーザー処置 (SIM User Action)	16003	ユーザーが SIM モジュールでプロセス (バックアップの開始やレポートの生成など) を開始したことを示します。	3
作成されたセッション (Session Created)	16004	ユーザー・セッションが作成されたことを示します。	3
破棄されたセッション (Session Destroyed)	16005	ユーザー・セッションが破棄されたことを示します。	3
作成された管理セッション (Admin Session Created)	16006	管理セッションが作成されたことを示します。	
破棄された管理セッション (Admin Session Destroyed)	16007	管理セッションが破棄されたことを示します。	3
無効なセッション認証 (Session Authentication Invalid)	16008	無効なセッション認証を示します。	5
有効期限が切れたセッション認証 (Session Authentication Expired)	16009	有効期限が切れたセッション認証を示します。	3
リスク・マネージャーの構成 (Risk Manager Configuration)	16010	ユーザーが IBM Security QRadar Risk Manager の構成を変更したことを示します。	3

VIS ホスト・ディスカバリー

VIS コンポーネントは、ネットワークで検出された新しいホスト、ポート、または脆弱性をディスカバーして保管したときに、イベントを生成します。これらのイベントは、その他のセキュリティー・イベントと相関するイベント・コレクターに送信されます。

以下の表で、VIS ホスト・ディスカバリー・カテゴリーの下位イベント・カテゴリーとそれに関連する重大度レベルについて説明します。

表 *97. VIS* ホスト・ディスカバリー・カテゴリーの下位イベント・カテゴリーと重大度レベル

下位イベント・カテゴリー	カテゴリー **ID**	説明	重大度レベル **(0** から **10** まで**)**
ディスカバーされた新規ホスト (New Host Discovered)	17001	VIS コンポーネントが新規ホストを検出したことを示します。	3
ディスカバーされた新規ポート (New Port Discovered)	17002	開いている新規ポートを VIS コンポーネントが検出したことを示します。	3
ディスカバーされた新しい脆弱性 (New Vuln Discovered)	17003	新しい脆弱性を VIS コンポーネントが検出したことを示します。	3
ディスカバーされた新しい OS (New OS Discovered)	17004	VIS コンポーネントがホストで新しいオペレーティング・システムを検出したことを示します。	3
ディスカバーされた大量のホスト (Bulk Host Discovered)	17005	VIS コンポーネントが短時間に多数の新規ホストを検出したことを示します。	3

アプリケーション

アプリケーション・カテゴリーには、E メール・アクティビティーや FTP アクティビティーなどの、アプリケーション・アクティビティーに関連するイベントが含まれます。

以下の表で、アプリケーション・カテゴリーの下位イベント・カテゴリーおよび関連する重大度レベルを説明します。

表 98. アプリケーション・カテゴリーの下位カテゴリーおよび重大度レベル

下位イベント・カテゴリー	カテゴリー ID	説明	重大度レベル (0 から 10 まで)
開かれたメール (Mail Opened)	18001	E メール接続が確立されたことを示します。	1
閉じられたメール (Mail Closed)	18002	E メール接続が閉じられたことを示します。	1
リセットされたメール (Mail Reset)	18003	E メール接続がリセットされたことを示します。	3
終了したメール (Mail Terminated)	18004	E メール接続が終了したことを示します。	4
拒否されたメール (Mail Denied)	18005	E メール接続が拒否されたことを示します。	4
進行中のメール (Mail in Progress)	18006	E メール接続が試行されていることを示します。	1
遅延したメール (Mail Delayed)	18007	E メール接続が遅延したことを示します。	4
キューに入れられたメール (Mail Queued)	18008	E メール接続がキューに入れられたことを示します。	3
リダイレクトされたメール (Mail Redirected)	18009	E メール接続がリダイレクトされたことを示します。	1
開かれた FTP (FTP Opened)	18010	FTP 接続が開かれたことを示します。	1
閉じられた FTP (FTP Closed)	18011	FTP 接続が閉じられたことを示します。	1
リセットされた FTP (FTP Reset)	18012	FTP 接続がリセットされたことを示します。	3
終了した FTP (FTP Terminated)	18013	FTP 接続が終了したことを示します。	4
拒否された FTP (FTP Denied)	18014	FTP 接続が拒否されたことを示します。	4
進行中の FTP (FTP In Progress)	18015	FTP 接続が進行中であることを示します。	1
リダイレクトされた FTP (FTP Redirected)	18016	FTP 接続がリダイレクトされたことを示します。	3

表 98. アプリケーション・カテゴリーの下位カテゴリーおよび重大度レベル (続き)

下位イベント・カテゴリー	カテゴリー ID	説明	重大度レベル (0 から 10 まで)
開かれた HTTP (HTTP Opened)	18017	HTTP 接続が確立されたことを示します。	1
閉じられた HTTP (HTTP Closed)	18018	HTTP 接続が閉じられたことを示します。	1
リセットされた HTTP (HTTP Reset)	18019	HTTP 接続がリセットされたことを示します。	3
終了した HTTP (HTTP Terminated)	18020	HTTP 接続が終了したことを示します。	4
拒否された HTTP (HTTP Denied)	18021	HTTP 接続が拒否されたことを示します。	4
進行中の HTTP (HTTP In Progress)	18022	HTTP 接続が進行中であることを示します。	1
遅延した HTTP (HTTP Delayed)	18023	HTTP 接続が遅延したことを示します。	3
キューに入れられた HTTP (HTTP Queued)	18024	HTTP 接続がキューに入れられたことを示します。	1
リダイレクトされた HTTP (HTTP Redirected)	18025	HTTP 接続がリダイレクトされたことを示します。	1
HTTP プロキシー (HTTP Proxy)	18026	HTTP 接続がプロキシー処理されていることを示します。	1
開かれた HTTPS (HTTPS Opened)	18027	HTTPS 接続が確立されたことを示します。	1
閉じられた HTTPS (HTTPS Closed)	18028	HTTPS 接続が閉じられたことを示します。	1
リセットされた HTTPS (HTTPS Reset)	18029	HTTPS 接続がリセットされたことを示します。	3
終了した HTTPS (HTTPS Terminated)	18030	HTTPS 接続が終了したことを示します。	4
拒否された HTTPS (HTTPS Denied)	18031	HTTPS 接続が拒否されたことを示します。	4

表 98. アプリケーション・カテゴリーの下位カテゴリーおよび重大度レベル (続き)

下位イベント・カテゴリー	カテゴリー ID	説明	重大度レベル (0 から 10 まで)
進行中の HTTPS (HTTPS In Progress)	18032	HTTPS 接続が進行中であることを示します。	1
遅延した HTTPS (HTTPS Delayed)	18033	HTTPS 接続が遅延したことを示します。	3
キューに入れられた HTTPS (HTTPS Queued)	18034	HTTPS 接続がキューに入れられたことを示します。	3
リダイレクトされた HTTPS (HTTPS Redirected)	18035	HTTPS 接続がリダイレクトされたことを示します。	3
HTTPS プロキシー (HTTPS Proxy)	18036	HTTPS 接続がプロキシー処理されていることを示します。	1
開かれた SSH (SSH Opened)	18037	SSH 接続が確立されたことを示します。	1
閉じられた SSH (SSH Closed)	18038	SSH 接続が閉じられたことを示します。	1
リセットされた SSH (SSH Reset)	18039	SSH 接続がリセットされたことを示します。	3
終了した SSH (SSH Terminated)	18040	SSH 接続が終了したことを示します。	4
拒否された SSH (SSH Denied)	18041	SSH セッションが拒否されたことを示します。	4
進行中の SSH (SSH In Progres)	18042	SSH セッションが進行中であることを示します。	1
開かれたリモート・アクセス (RemoteAccess Opened)	18043	リモート・アクセス接続が確立されたことを示します。	1
閉じられたリモート・アクセス (RemoteAccess Closed)	18044	リモート・アクセス接続が閉じられたことを示します。	1
リセットされたリモート・アクセス (RemoteAccess Reset)	18045	リモート・アクセス接続がリセットされたことを示します。	3
終了したリモート・アクセス (RemoteAccess Terminated)	18046	リモート・アクセス接続が終了したことを示します。	4

表 98. アプリケーション・カテゴリーの下位カテゴリーおよび重大度レベル (続き)

下位イベント・カテゴリー	カテゴリー ID	説明	重大度レベル (0 から 10 まで)
拒否されたリモート・アクセス (RemoteAccess Denied)	18047	リモート・アクセス接続が拒否されたことを示します。	4
進行中のリモート・アクセス (RemoteAccess In Progress)	18048	リモート・アクセス接続が進行中であることを示します。	1
リモート・アクセス遅延	18049	リモート・アクセス接続が遅延したことを示します。	3
リダイレクトされたリモート・アクセス (RemoteAccess Redirected)	18050	リモート・アクセス接続がリダイレクトされたことを示します。	3
開かれた VPN (VPN Opened)	18051	VPN 接続が開かれたことを示します。	1
閉じられた VPN (VPN Closed)	18052	VPN 接続が閉じられたことを示します。	1
リセットされた VPN (VPN Reset)	18053	VPN 接続がリセットされたことを示します。	3
終了した VPN (VPN Terminated)	18054	VPN 接続が終了したことを示します。	4
拒否された VPN (VPN Denied)	18055	VPN 接続が拒否されたことを示します。	4
進行中の VPN (VPN In Progress)	18056	VPN 接続が進行中であることを示します。	1
遅延した VPN (VPN Delayed)	18057	VPN 接続が遅延したことを示します。	3
キューに入れられた VPN (VPN Queued)	18058	VPN 接続がキューに入れられたことを示します。	3
リダイレクトされた VPN (VPN Redirected)	18059	VPN 接続がリダイレクトされたことを示します。	3
開かれた RDP (RDP Opened)	18060	RDP 接続が確立されたことを示します。	1
閉じられた RDP (RDP Closed)	18061	RDP 接続が閉じられたことを示します。	1
リセットされた RDP (RDP Reset)	18062	RDP 接続がリセットされたことを示します。	3

表 98. アプリケーション・カテゴリーの下位カテゴリーおよび重大度レベル (続き)

下位イベント・カテゴリー	カテゴリー ID	説明	重大度レベル (0 から 10 まで)
終了した RDP (RDP Terminated)	18063	RDP 接続が終了したことを示します。	4
拒否された RDP (RDP Denied)	18064	RDP 接続が拒否されたことを示します。	4
進行中の RDP (RDP In Progress)	18065	RDP 接続が進行中であることを示します。	1
リダイレクトされた RDP (RDP Redirected)	18066	RDP 接続がリダイレクトされたことを示します。	3
開かれたファイル転送 (FileTransfer Opened)	18067	ファイル転送接続が確立されたことを示します。	1
閉じられたファイル転送 (FileTransfer Closed)	18068	ファイル転送接続が閉じられたことを示します。	1
リセットされたファイル転送 (FileTransfer Reset)	18069	ファイル転送接続がリセットされたことを示します。	3
終了したファイル転送 (FileTransfer Terminated)	18070	ファイル転送接続が終了したことを示します。	4
拒否されたファイル転送 (FileTransfer Denied)	18071	ファイル転送接続が拒否されたことを示します。	4
進行中のファイル転送 (FileTransfer In Progress)	18072	ファイル転送接続が進行中であることを示します。	1
遅延したファイル転送 (FileTransfer Delayed)	18073	ファイル転送接続が遅延したことを示します。	3
キューに入れられたファイル転送 (FileTransfer Queued)	18074	ファイル転送接続がキューに入れられたことを示します。	3
ファイル転送リダイレクト	18075	ファイル転送接続がリダイレクトされたことを示します。	3
開かれた DNS (DNS Opened)	18076	DNS 接続が確立されたことを示します。	1
閉じられた DNS (DNS Closed)	18077	DNS 接続が閉じられたことを示します。	1

表 98. アプリケーション・カテゴリーの下位カテゴリーおよび重大度レベル (続き)

下位イベント・カテゴリー	カテゴリー ID	説明	重大度レベル (0 から 10 まで)
リセットされた DNS (DNS Reset)	18078	DNS 接続がリセットされたことを示します。	5
終了した DNS (DNS Terminated)	18079	DNS 接続が終了したことを示します。	5
拒否された DNS (DNS Denied)	18080	DNS 接続が拒否されたことを示します。	5
進行中の DNS (DNS In Progress)	18081	DNS 接続が進行中であることを示します。	1
遅延した DNS (DNS Delayed)	18082	DNS 接続が遅延したことを示します。	5
リダイレクトされた DNS (DNS Redirected)	18083	DNS 接続がリダイレクトされたことを示します。	4
開かれたチャット (Chat Opened)	18084	チャット接続が開かれたことを示します。	1
閉じられたチャット (Chat Closed)	18085	チャット接続が閉じられたことを示します。	1
リセットされたチャット (Chat Reset)	18086	チャット接続がリセットされたことを示します。	3
チャット終了	18087	チャット接続が終了したことを示します。	3
拒否されたチャット (Chat Denied)	18088	チャット接続が拒否されたことを示します。	3
進行中のチャット (Chat In Progress)	18089	チャット接続が進行中であることを示します。	1
リダイレクトされたチャット (Chat Redirected)	18090	チャット接続がリダイレクトされたことを示します。	1
開かれたデータベース (Database Opened)	18091	データベース接続が確立されたことを示します。	1
データベースのクローズ	18092	データベース接続が閉じられたことを示します。	1

表 98. アプリケーション・カテゴリーの下位カテゴリーおよび重大度レベル (続き)

下位イベント・カテゴリー	カテゴリー ID	説明	重大度レベル (0 から 10 まで)
リセットされたデータベース (Database Reset)	18093	データベース接続がリセットされたことを示します。	5
終了したデータベース (Database Terminated)	18094	データベース接続が終了したことを示します。	5
拒否されたデータベース (Database Denied)	18095	データベース接続が拒否されたことを示します。	5
進行中のデータベース (Database In Progress)	18096	データベース接続が進行中であることを示します。	1
リダイレクトされたデータベース (Database Redirected)	18097	データベース接続がリダイレクトされたことを示します。	3
開かれた SMTP (SMTP Opened)	18098	SMTP 接続が確立されたことを示します。	1
SMTP クローズ	18099	SMTP 接続が閉じられたことを示します。	1
リセットされた SMTP (SMTP Reset)	18100	SMTP 接続がリセットされたことを示します。	3
終了した SMTP (SMTP Terminated)	18101	SMTP 接続が終了したことを示します。	5
拒否された SMTP (SMTP Denied)	18102	SMTP 接続が拒否されたことを示します。	5
進行中の SMTP (SMTP In Progress)	18103	SMTP 接続が進行中であることを示します。	1
遅延した SMTP (SMTP Delayed)	18104	SMTP 接続が遅延したことを示します。	3
キューに入れられた SMTP (SMTP Queued)	18105	SMTP 接続がキューに入れられたことを示します。	3
リダイレクトされた SMTP (SMTP Redirected)	18106	SMTP 接続がリダイレクトされたことを示します。	3
開かれた許可 (Auth Opened)	18107	許可サーバー接続が確立されたことを示します。	1

表 98. アプリケーション・カテゴリーの下位カテゴリーおよび重大度レベル (続き)

下位イベント・カテゴリー	カテゴリー ID	説明	重大度レベル (0 から 10 まで)
閉じられた許可 (Auth Closed)	18108	許可サーバー接続が閉じられたことを示します。	1
リセットされた許可 (Auth Reset)	18109	許可サーバー接続がリセットされたことを示します。	3
終了した許可 (Auth Terminated)	18110	許可サーバー接続が終了したことを示します。	4
拒否された許可 (Auth Denied)	18111	許可サーバー接続が拒否されたことを示します。	4
進行中の許可 (Auth In Progress)	18112	許可サーバー接続が進行中であることを示します。	1
遅延した許可 (Auth Delayed)	18113	許可サーバー接続が遅延したことを示します。	3
キューに入れられた許可 (Auth Queued)	18114	許可サーバー接続がキューに入れられたことを示します。	3
リダイレクトされた許可 (Auth Redirected)	18115	許可サーバー接続がリダイレクトされたことを示します。	2
開かれた P2P (P2P Opened)	18116	対等通信 (P2P) 接続が確立されたことを示します。	1
閉じられた P2P (P2P Closed)	18117	P2P 接続が閉じられたことを示します。	1
リセットされた P2P (P2P Reset)	18118	P2P 接続がリセットされたことを示します。	4
終了した P2P (P2P Terminated)	18119	P2P 接続が終了したことを示します。	4
拒否された P2P (P2P Denied)	18120	P2P 接続が拒否されたことを示します。	3
進行中の P2P (P2P In Progress)	18121	P2P 接続が進行中であることを示します。	1
開かれた Web (Web Opened)	18122	Web 接続が確立されたことを示します。	1
閉じられた Web (Web Closed)	18123	Web 接続が閉じられたことを示します。	1

表 98. アプリケーション・カテゴリーの下位カテゴリーおよび重大度レベル (続き)

下位イベント・カテゴリー	カテゴリー ID	説明	重大度レベル (0 から 10 まで)
リセットされた Web (Web Reset)	18124	Web 接続がリセットされたことを示します。	4
終了した Web (Web Terminated)	18125	Web 接続が終了したことを示します。	4
拒否された Web (Web Denied)	18126	Web 接続が拒否されたことを示します。	4
進行中の Web (Web In Progress)	18127	Web 接続が進行中であることを示します。	1
遅延した Web (Web Delayed)	18128	Web 接続が遅延したことを示します。	3
キューに入れられた Web (Web Queued)	18129	Web 接続がキューに入れられたことを示します。	1
リダイレクトされた Web (Web Redirected)	18130	Web 接続がリダイレクトされたことを示します。	1
Web プロキシー (Web Proxy)	18131	Web 接続がプロキシー処理されたことを示します。	1
開かれた VoIP (VoIP Opened)	18132	Voice Over IP (VoIP) 接続が確立されたことを示します。	1
閉じられた VoIP (VoIP Closed)	18133	VoIP 接続が閉じられたことを示します。	1
リセットされた VoIP (VoIP Reset)	18134	VoIP 接続がリセットされたことを示します。	3
終了した VoIP (VoIP Terminated)	18135	VoIP 接続が終了したことを示します。	3
拒否された VoIP (VoIP Denied)	18136	VoIP 接続が拒否されたことを示します。	3
進行中の VoIP (VoIP In Progress)	18137	VoIP 接続が進行中であることを示します。	1
遅延した VoIP (VoIP Delayed)	18138	VoIP 接続が遅延したことを示します。	3
リダイレクトされた VoIP (VoIP Redirected)	18139	VoIP 接続がリダイレクトされたことを示します。	3

表 98. アプリケーション・カテゴリーの下位カテゴリーおよび重大度レベル (続き)

下位イベント・カテゴリー	カテゴリー ID	説明	重大度レベル (0 から 10 まで)
開始された LDAP セッション (LDAP Session Started)	18140	LDAP セッションが開始されたことを示します。	1
終了した LDAP セッション (LDAP Session Ended)	18141	LDAP セッションが終了したことを示します。	1
拒否された LDAP セッション (LDAP Session Denied)	18142	LDAP セッションが拒否されたことを示します。	3
LDAP セッション状況 (LDAP Session Status)	18143	LDAP セッション状況メッセージが報告されたことを示します。	1
失敗した LDAP 認証 (LDAP Authentication Failed)	18144	LDAP 認証が失敗したことを示します。	4
成功した LDAP 認証 (LDAP Authentication Succeeded)	18145	LDAP 認証が成功したことを示します。	1
開始された AAA セッション (AAA Session Started)	18146	認証、許可、および会計 (AAA) セッションが開始されたことを示します。	1
終了した AAA セッション (AAA Session Ended)	18147	AAA セッションが終了したことを示します。	1
拒否された AAA セッション (AAA Session Denied)	18148	AAA セッションが拒否されたことを示します。	3
AAA セッション状況 (AAA Session Status)	18149	AAA セッション状況メッセージが報告されたことを示します。	1
失敗した AAA 認証 (AAA Authentication Failed)	18150	AAA 認証が失敗したことを示します。	4
成功した AAA 認証 (AAA Authentication Succeeded)	18151	AAA 認証が成功したことを示します。	1

表 98. アプリケーション・カテゴリーの下位カテゴリーおよび重大度レベル (続き)

下位イベント・カテゴリー	カテゴリー ID	説明	重大度レベル (0 から 10 まで)
失敗した IPSEC 認証 (IPSEC Authentication Failed)	18152	インターネット・プロトコル・セキュリティー (IPSEC) 認証が失敗したことを示します。	4
成功した IPSEC 認証 (IPSEC Authentication Succeeded)	18153	IPSEC 認証が成功したことを示します。	1
開始された IPSEC セッション (IPSEC Session Started)	18154	IPSEC セッションが開始されたことを示します。	1
終了した IPSEC セッション (IPSEC Session Ended)	18155	IPSEC セッションが終了したことを示します。	1
IPSEC エラー (IPSEC Error)	18156	IPSEC エラー・メッセージが報告されたことを示します。	5
IPSEC 状況 (IPSEC Status)	18157	IPSEC セッション状況メッセージが報告されたことを示します。	1
開かれた IM セッション (IM Session Opened)	18158	インスタント・メッセンジャー (IM) セッションが確立されたことを示します。	1
閉じられた IM セッション (IM Session Closed)	18159	IM セッションが閉じられたことを示します。	1
リセットされた IM セッション (IM Session Reset)	18160	IM セッションがリセットされたことを示します。	3
終了した IM セッション (IM Session Terminated)	18161	IM セッションが終了したことを示します。	3
拒否された IM セッション (IM Session Denied)	18162	IM セッションが拒否されたことを示します。	3
進行中の IM セッション (IM Session In Progress)	18163	IM セッションが進行中であることを示します。	1
遅延した IM セッション (IM Session Delayed)	18164	IM セッションが遅延したことを示します	3

表 98. アプリケーション・カテゴリーの下位カテゴリーおよび重大度レベル (続き)

下位イベント・カテゴリー	カテゴリー ID	説明	重大度レベル (0 から 10 まで)
リダイレクトされた IM セッション (IM Session Redirected)	18165	IM セッションがリダイレクトされたことを示します。	3
開かれた WHOIS セッション (WHOIS Session Opened)	18166	WHOIS セッションが確立されたことを示します。	1
閉じられた WHOIS セッション (WHOIS Session Closed)	18167	WHOIS セッションが閉じられたことを示します。	1
リセットされた WHOIS セッション (WHOIS Session Reset)	18168	WHOIS セッションがリセットされたことを示します。	3
終了した WHOIS セッション (WHOIS Session Terminated)	18169	WHOIS セッションが終了したことを示します。	3
拒否された WHOIS セッション (WHOIS Session Denied)	18170	WHOIS セッションが拒否されたことを示します。	3
進行中の WHOIS セッション (WHOIS Session In Progress)	18171	WHOIS セッションが進行中であることを示します。	1
リダイレクトされた WHOIS セッション (WHOIS Session Redirected)	18172	WHOIS セッションがリダイレクトされたことを示します。	3
開かれたトレース・ルート・セッション (Traceroute Session Opened)	18173	トレース・ルート・セッションが確立されたことを示します。	1
閉じられたトレース・ルート・セッション (Traceroute Session Closed)	18174	トレース・ルート・セッションが閉じられたことを示します。	1
拒否されたトレース・ルート・セッション (Traceroute Session Denied)	18175	トレース・ルート・セッションが拒否されたことを示します。	3
進行中のトレース・ルート・セッション (Traceroute Session In Progress)	18176	トレース・ルート・セッションが進行中であることを示します。	1

表 98. アプリケーション・カテゴリーの下位カテゴリーおよび重大度レベル (続き)

下位イベント・カテゴリー	カテゴリー ID	説明	重大度レベル (0 から 10 まで)
開かれた TN3270 セッション (TN3270 Session Opened)	18177	TN3270 は、IBM 3270 端末に接続するために使用される端末エミュレーション・プログラムです。このカテゴリーは、TN3270 セッションが確立されたことを示します。	1
閉じられた TN3270 セッション (TN3270 Session Closed)	18178	TN3270 セッションが閉じられたことを示します。	1
リセットされた TN3270 セッション (TN3270 Session Reset)	18179	TN3270 セッションがリセットされたことを示します。	3
終了した TN3270 セッション (TN3270 Session Terminated)	18180	TN3270 セッションが終了したことを示します。	3
拒否された TN3270 セッション (TN3270 Session Denied)	18181	TN3270 セッションが拒否されたことを示します。	3
進行中の TN3270 セッション (TN3270 Session In Progress)	18182	TN3270 セッションが進行中であることを示します。	1
開かれた TFTP セッション (TFTP Session Opened)	18183	TFTP セッションが確立されたことを示します。	1
閉じられた TFTP セッション (TFTP Session Closed)	18184	TFTP セッションが閉じられたことを示します。	1
リセットされた TFTP セッション (TFTP Session Reset)	18185	TFTP セッションがリセットされたことを示します。	3
終了した TFTP セッション (TFTP Session Terminated)	18186	TFTP セッションが終了したことを示します。	3
拒否された TFTP セッション (TFTP Session Denied)	18187	TFTP セッションが拒否されたことを示します。	3
進行中の TFTP セッション (TFTP Session In Progress)	18188	TFTP セッションが進行中であることを示します。	1

表 98. アプリケーション・カテゴリーの下位カテゴリーおよび重大度レベル (続き)

下位イベント・カテゴリー	カテゴリー ID	説明	重大度レベル (0 から 10 まで)
開かれた Telnet セッション (Telnet Session Opened)	18189	Telnet セッションが確立されたことを示します。	1
閉じられた Telnet セッション (Telnet Session Closed)	18190	Telnet セッションが閉じられたことを示します。	1
リセットされた Telnet セッション (Telnet Session Reset)	18191	Telnet セッションがリセットされたことを示します。	3
終了した Telnet セッション (Telnet Session Terminated)	18192	Telnet セッションが終了したことを示します。	3
拒否された Telnet セッション (Telnet Session Denied)	18193	Telnet セッションが拒否されたことを示します。	3
進行中の Telnet セッション (Telnet Session In Progress)	18194	Telnet セッションが進行中であることを示します。	1
開かれた Syslog セッション (Syslog Session Opened)	18201	Syslog セッションが確立されたことを示します。	1
閉じられた Syslog セッション (Syslog Session Closed)	18202	Syslog セッションが閉じられたことを示します。	1
拒否された Syslog セッション (Syslog Session Denied)	18203	Syslog セッションが拒否されたことを示します。	3
進行中の Syslog セッション (Syslog Session In Progress)	18204	Syslog セッションが進行中であることを示します。	1
開かれた SSL セッション (SSL Session Opened)	18205	Secure Socket Layer (SSL) セッションが確立されたことを示します。	1
閉じられた SSL セッション (SSL Session Closed)	18206	SSL セッションが閉じられたことを示します。	1
リセットされた SSL セッション (SSL Session Reset)	18207	SSL セッションがリセットされたことを示します。	3
終了した SSL セッション (SSL Session Terminated)	18208	SSL セッションが終了したことを示します。	3

表 98. アプリケーション・カテゴリーの下位カテゴリーおよび重大度レベル (続き)

下位イベント・カテゴリー	カテゴリー ID	説明	重大度レベル (0 から 10 まで)
拒否された SSL セッション (SSL Session Denied)	18209	SSL セッションが拒否されたことを示します。	3
進行中の SSL セッション (SSL Session In Progress)	18210	SSL セッションが進行中であることを示します。	1
開かれた SNMP セッション (SNMP Session Opened)	18211	Simple Network Management Protocol (SNMP) セッションが確立されたことを示します。	1
閉じられた SNMP セッション (SNMP Session Closed)	18212	SNMP セッションが閉じられたことを示します。	1
拒否された SNMP セッション (SNMP Session Denied)	18213	SNMP セッションが拒否されたことを示します。	3
進行中の SNMP セッション (SNMP Session In Progress)	18214	SNMP セッションが進行中であることを示します。	1
開かれた SMB セッション (SMB Session Opened)	18215	Server Message Block (SMB) セッションが確立されたことを示します。	1
閉じられた SMB セッション (SMB Session Closed)	18216	SMB セッションが閉じられたことを示します。	1
リセットされた SMB セッション (SMB Session Reset)	18217	SMB セッションがリセットされたことを示します。	3
終了した SMB セッション (SMB Session Terminated)	18218	SMB セッションが終了したことを示します。	3
拒否された SMB セッション (SMB Session Denied)	18219	SMB セッションが拒否されたことを示します。	3
進行中の SMB セッション (SMB Session In Progress)	18220	SMB セッションが進行中であることを示します。	1
開かれたストリーミング・メディア・セッション (Streaming Media Session Opened)	18221	ストリーミング・メディア・セッションが確立されたことを示します。	1

表 98. アプリケーション・カテゴリーの下位カテゴリーおよび重大度レベル (続き)

下位イベント・カテゴリー	カテゴリー ID	説明	重大度レベル (0 から 10 まで)
閉じられたストリーミング・メディア・セッション (Streaming Media Session Closed)	18222	ストリーミング・メディア・セッションが閉じられたことを示します。	1
リセットされたストリーミング・メディア・セッション (Streaming Media Session Reset)	18223	ストリーミング・メディア・セッションがリセットされたことを示します。	3
終了したストリーミング・メディア・セッション (Streaming Media Session Terminated)	18224	ストリーミング・メディア・セッションが終了したことを示します。	3
拒否されたストリーミング・メディア・セッション (Streaming Media Session Denied)	18225	ストリーミング・メディア・セッションが拒否されたことを示します。	3
進行中のストリーミング・メディア・セッション (Streaming Media Session In Progress)	18226	ストリーミング・メディア・セッションが進行中であることを示します。	1
開かれた RUSERS セッション (RUSERS Session Opened)	18227	(リモート・ユーザー) RUSERS セッションが確立されたことを示します。	1
閉じられた RUSERS セッション (RUSERS Session Closed)	18228	RUSERS セッションが閉じられたことを示します。	1
拒否された RUSERS セッション (RUSERS Session Denied)	18229	RUSERS セッションが拒否されたことを示します。	3
進行中の RUSERS セッション (RUSERS Session In Progress)	18230	RUSERS セッションが進行中であることを示します。	1
開かれた Rsh セッション (Rsh Session Opened)	18231	リモート・シェル (Rsh) セッションが確立されたことを示します。	1
閉じられた Rsh セッション (Rsh Session Closed)	18232	Rsh セッションが閉じられたことを示します。	1

表 98. アプリケーション・カテゴリーの下位カテゴリーおよび重大度レベル (続き)

下位イベント・カテゴリー	カテゴリー ID	説明	重大度レベル (0 から 10 まで)
リセットされた Rsh セッション (Rsh Session Reset)	18233	Rsh セッションがリセットされたことを示します。	3
終了した Rsh セッション (Rsh Session Terminated)	18234	Rsh セッションが終了したことを示します。	3
拒否された Rsh セッション (Rsh Session Denied)	18235	Rsh セッションが拒否されたことを示します。	3
進行中の Rsh セッション (Rsh Session In Progress)	18236	Rsh セッションが進行中であることを示します。	1
開かれた RLOGIN セッション (RLOGIN Session Opened)	18237	リモート・ログイン (RLOGIN) セッションが確立されたことを示します。	1
閉じられた RLOGIN セッション (RLOGIN Session Closed)	18238	RLOGIN セッションが閉じられたことを示します。	1
リセットされた RLOGIN セッション (RLOGIN Session Reset)	18239	RLOGIN セッションがリセットされたことを示します。	3
終了した RLOGIN セッション (RLOGIN Session Terminated)	18240	RLOGIN セッションが終了したことを示します。	3
拒否された RLOGIN セッション (RLOGIN Session Denied)	18241	RLOGIN セッションが拒否されたことを示します。	3
進行中の RLOGIN セッション (RLOGIN Session In Progress)	18242	RLOGIN セッションが進行中であることを示します。	1
開かれた REXEC セッション (REXEC Session Opened)	18243	(リモート実行) REXEC セッションが確立されたことを示します。	1
閉じられた REXEC セッション (REXEC Session Closed)	18244	REXEC セッションが閉じられたことを示します。	1
リセットされた REXEC セッション (REXEC Session Reset)	18245	REXEC セッションがリセットされたことを示します。	3

表 98. アプリケーション・カテゴリーの下位カテゴリーおよび重大度レベル (続き)

下位イベント・カテゴリー	カテゴリー ID	説明	重大度レベル (0 から 10 まで)
終了した REXEC セッション (REXEC Session Terminated)	18246	REXEC セッションが終了したことを示します。	3
拒否された REXEC セッション (REXEC Session Denied)	18247	REXEC セッションが拒否されたことを示します。	3
進行中の REXEC セッション (REXEC Session In Progress)	18248	REXEC セッションが進行中であることを示します。	1
開かれた RPC セッション (RPC Session Opened)	18249	リモート・プロシージャー・コール (RPC) セッションが確立されたことを示します。	1
閉じられた RPC セッション (RPC Session Closed)	18250	RPC セッションが閉じられたことを示します。	1
リセットされた RPC セッション (RPC Session Reset)	18251	RPC セッションがリセットされたことを示します。	3
終了した RPC セッション (RPC Session Terminated)	18252	RPC セッションが終了したことを示します。	3
拒否された RPC セッション (RPC Session Denied)	18253	RPC セッションが拒否されたことを示します。	3
進行中の RPC セッション (RPC Session In Progres)	18254	RPC セッションが進行中であることを示します。	1
開かれた NTP セッション (NTP Session Opened)	18255	Network Time Protocol (NTP) セッションが確立されたことを示します。	1
閉じられた NTP セッション (NTP Session Closed)	18256	NTP セッションが閉じられたことを示します。	1
リセットされた NTP セッション (NTP Session Reset)	18257	NTP セッションがリセットされたことを示します。	3
終了した NTP セッション (NTP Session Terminated)	18258	NTP セッションが終了したことを示します。	3
拒否された NTP セッション (NTP Session Denied)	18259	NTP セッションが拒否されたことを示します。	3

表 98. アプリケーション・カテゴリーの下位カテゴリーおよび重大度レベル (続き)

下位イベント・カテゴリー	カテゴリー ID	説明	重大度レベル (0 から 10 まで)
進行中の NTP セッション (NTP Session In Progress)	18260	NTP セッションが進行中であることを示します。	1
開かれた NNTP セッション (NNTP Session Opened)	18261	ネットワーク・ニュース転送プロトコル (NNTP) セッションが確立されたことを示します。	1
閉じられた NNTP セッション (NNTP Session Closed)	18262	NNTP セッションが閉じられたことを示します。	1
リセットされた NNTP セッション (NNTP Session Reset)	18263	NNTP セッションがリセットされたことを示します。	3
終了した NNTP セッション (NNTP Session Terminated)	18264	NNTP セッションが終了したことを示します。	3
拒否された NNTP セッション (NNTP Session Denied)	18265	NNTP セッションが拒否されたことを示します。	3
進行中の NNTP セッション (NNTP Session In Progress)	18266	NNTP セッションが進行中であることを示します。	1
開かれた NFS セッション (NFS Session Opened)	18267	ネットワーク・ファイル・システム (NFS) セッションが確立されたことを示します。	1
閉じられた NFS セッション (NFS Session Closed)	18268	NFS セッションが閉じられたことを示します。	1
NFS セッションのリセット	18269	NFS セッションがリセットされたことを示します。	3
終了した NFS セッション (NFS Session Terminate)	18270	NFS セッションが終了したことを示します。	3
拒否された NFS セッション (NFS Session Denied)	18271	NFS セッションが拒否されたことを示します。	3
進行中の NFS セッション (NFS Session In Progress)	18272	NFS セッションが進行中であることを示します。	1

表 98. アプリケーション・カテゴリーの下位カテゴリーおよび重大度レベル (続き)

下位イベント・カテゴリー	カテゴリー ID	説明	重大度レベル (0 から 10 まで)
開かれた NCP セッション (NCP Session Opened)	18273	ネットワーク制御プログラム (NCP) セッションが確立されたことを示します。	1
閉じられた NCP セッション (NCP Session Closed)	18274	NCP セッションが閉じられたことを示します。	1
リセットされた NCP セッション (NCP Session Reset)	18275	NCP セッションがリセットされたことを示します。	3
終了した NCP セッション (NCP Session Terminated)	18276	NCP セッションが終了したことを示します。	3
拒否された NCP セッション (NCP Session Denied)	18277	NCP セッションが拒否されたことを示します。	3
進行中の NCP セッション (NCP Session In Progress)	18278	NCP セッションが進行中であることを示します。	1
開かれた NetBIOS セッション (NetBIOS Session Opened)	18279	NetBIOS セッションが確立されたことを示します。	1
閉じられた NetBIOS セッション (NetBIOS Session Closed)	18280	NetBIOS セッションが閉じられたことを示します。	1
リセットされた NetBIOS セッション (NetBIOS Session Reset)	18281	NetBIOS セッションがリセットされたことを示します。	3
終了した NetBIOS セッション (NetBIOS Session Terminated)	18282	NetBIOS セッションが終了したことを示します。	3
拒否された NetBIOS セッション (NetBIOS Session Denied)	18283	NetBIOS セッションが拒否されたことを示します。	3
進行中の NetBIOS セッション (NetBIOS Session In Progress)	18284	NetBIOS セッションが進行中であることを示します。	1
開かれた MODBUS セッション (MODBUS Session Opened)	18285	MODBUS セッションが確立されたことを示します。	1

表 98. アプリケーション・カテゴリーの下位カテゴリーおよび重大度レベル (続き)

下位イベント・カテゴリー	カテゴリー ID	説明	重大度レベル (0 から 10 まで)
閉じられた MODBUS セッション (MODBUS Session Closed)	18286	MODBUS セッションが閉じられたことを示します。	1
リセットされた MODBUS セッション (MODBUS Session Reset)	18287	MODBUS セッションがリセットされたことを示します。	3
終了した MODBUS セッション (MODBUS Session Terminated)	18288	MODBUS セッションが終了したことを示します。	3
拒否された MODBUS セッション (MODBUS Session Denied)	18289	MODBUS セッションが拒否されたことを示します。	3
進行中の MODBUS セッション (MODBUS Session In Progress)	18290	MODBUS セッションが進行中であることを示します。	1
開かれた LPD セッション (LPD Session Opened)	18291	ライン・プリンター・デーモン (LPD) セッションが確立されたことを示します。	1
閉じられた LPD セッション (LPD Session Closed)	18292	LPD セッションが閉じられたことを示します。	1
リセットされた LPD セッション (LPD Session Reset)	18293	LPD セッションがリセットされたことを示します。	3
終了した LPD セッション (LPD Session Terminated)	18294	LPD セッションが終了したことを示します。	3
拒否された LPD セッション (LPD Session Denied)	18295	LPD セッションが拒否されたことを示します。	3
進行中の LPD セッション (LPD Session In Progress)	18296	LPD セッションが進行中であることを示します。	1
Lotus Notes® セッションのオープン	18297	Lotus Notes セッションが確立されたことを示します。	1

表 98. アプリケーション・カテゴリーの下位カテゴリーおよび重大度レベル (続き)

下位イベント・カテゴリー	カテゴリー ID	説明	重大度レベル (0 から 10 まで)
Lotus Notes セッションのクローズ	18298	Lotus Notes セッションが閉じられたことを示します。	1
Lotus Notes セッションのリセット	18299	Lotus Notes セッションがリセットされたことを示します。	3
Lotus Notes セッション終了	18300	Lotus Notes セッションが終了したことを示します。	3
Lotus Notes セッション拒否	18301	Lotus Notes セッションが拒否されたことを示します。	3
Lotus Notes セッション進行中	18302	Lotus Notes セッションが進行中であることを示します。	1
Kerberos セッションのオープン	18303	Kerberos セッションが確立されたことを示します。	1
閉じられた Kerberos セッション (Kerberos Session Closed)	18304	Kerberos セッションが閉じられたことを示します。	1
リセットされた Kerberos セッション (Kerberos Session Reset)	18305	Kerberos セッションがリセットされたことを示します。	3
終了した Kerberos セッション (Kerberos Session Terminated)	18306	Kerberos セッションが終了したことを示します。	3
拒否された Kerberos セッション (Kerberos Session Denied)	18307	Kerberos セッションが拒否されたことを示します。	3
進行中の Kerberos セッション (Kerberos Session In Progress)	18308	Kerberos セッションが進行中であることを示します。	1
開かれた IRC セッション (IRC Session Opened)	18309	インターネット中継チャット (IRC) セッションが確立されたことを示します。	1
閉じられた IRC セッション (IRC Session Closed)	18310	IRC セッションが閉じられたことを示します。	1
リセットされた IRC セッション (IRC Session Reset)	18311	IRC セッションがリセットされたことを示します。	3

表 98. アプリケーション・カテゴリーの下位カテゴリーおよび重大度レベル (続き)

下位イベント・カテゴリー	カテゴリー ID	説明	重大度レベル (0 から 10 まで)
終了した IRC セッション (IRC Session Terminated)	18312	IRC セッションが終了したことを示します。	3
拒否された IRC セッション (IRC Session Denied)	18313	IRC セッションが拒否されたことを示します。	3
進行中の IRC セッション (IRC Session In Progress)	18314	IRC セッションが進行中であることを示します。	1
開かれた IEC 104 セッション (IEC 104 Session Opened)	18315	IEC 104 セッションが確立されたことを示します。	1
閉じられた IEC 104 セッション (IEC 104 Session Closed)	18316	IEC 104 セッションが閉じられたことを示します。	1
リセットされた IEC 104 セッション (IEC 104 Session Reset)	18317	IEC 104 セッションがリセットされたことを示します。	3
終了した IEC 104 セッション (IEC 104 Session Terminated)	18318	IEC 104 セッションが終了したことを示します。	3
拒否された IEC 104 セッション (IEC 104 Session Denied)	18319	IEC 104 セッションが拒否されたことを示します。	3
進行中の IEC 104 セッション (IEC 104 Session In Progress)	18320	IEC 104 セッションが進行中であることを示します。	1
開かれた Ident セッション (Ident Session Opened)	18321	TCP Client Identity Protocol (Ident) セッションが確立されたことを示します。	1
閉じられた Ident セッション (Ident Session Closed)	18322	Ident セッションが閉じられたことを示します。	1
リセットされた Ident セッション (Ident Session Reset)	18323	Ident セッションがリセットされたことを示します。	3
終了した Ident セッション (Ident Session Terminated)	18324	Ident セッションが終了したことを示します。	3
拒否された Ident セッション (Ident Session Denied)	18325	Ident セッションが拒否されたことを示します。	3

表 98. アプリケーション・カテゴリーの下位カテゴリーおよび重大度レベル (続き)

下位イベント・カテゴリー	カテゴリー ID	説明	重大度レベル (0 から 10 まで)
進行中の Ident セッション (Ident Session In Progress)	18326	Ident セッションが進行中であることを示します。	1
開かれた ICCP セッション (ICCP Session Opened)	18327	Inter-Control Center Communications Protocol (ICCP) セッションが確立されたことを示します。	1
閉じられた ICCP セッション (ICCP Session Closed)	18328	ICCP セッションが閉じられたことを示します。	1
リセットされた ICCP セッション (ICCP Session Reset)	18329	ICCP セッションがリセットされたことを示します。	3
終了した ICCP セッション (ICCP Session Terminated)	18330	ICCP セッションが終了したことを示します。	3
拒否された ICCP セッション (ICCP Session Denied)	18331	ICCP セッションが拒否されたことを示します。	3
進行中の ICCP セッション (ICCP Session In Progress)	18332	ICCP セッションが進行中であることを示します。	1
GroupWise セッションのオープン	18333	GroupWise セッションが確立されたことを示します。	1
GroupWise セッションのクローズ	18334	GroupWise セッションが閉じられたことを示します。	1
GroupWise セッションのリセット	18335	GroupWise セッションがリセットされたことを示します。	3
GroupWise セッション終了	18336	GroupWise セッションが終了したことを示します。	3
GroupWise セッション拒否	18337	GroupWise セッションが拒否されたことを示します。	3
GroupWise セッション進行中	18338	GroupWise セッションが進行中であることを示します。	1
Gopher セッションのオープン	183398	Gopher セッションが確立されたことを示します。	1

表 98. アプリケーション・カテゴリーの下位カテゴリーおよび重大度レベル (続き)

下位イベント・カテゴリー	カテゴリー ID	説明	重大度レベル (0 から 10 まで)
閉じられた Gopher セッション (Gopher Session Closed)	18340	Gopher セッションが閉じられたことを示します。	1
リセットされた Gopher セッション (Gopher Session Reset)	18341	Gopher セッションがリセットされたことを示します。	3
終了した Gopher セッション (Gopher Session Terminated)	18342	Gopher セッションが終了したことを示します。	3
拒否された Gopher セッション (Gopher Session Denied)	18343	Gopher セッションが拒否されたことを示します。	3
進行中の Gopher セッション (Gopher Session In Progress)	18344	Gopher セッションが進行中であることを示します。	1
開かれた GIOP セッション (GIOP Session Opened)	18345	General Inter-ORB Protocol (GIOP) セッションが確立されたことを示します。	1
閉じられた GIOP セッション (GIOP Session Closed)	18346	GIOP セッションが閉じられたことを示します。	1
リセットされた GIOP セッション (GIOP Session Reset)	18347	GIOP セッションがリセットされたことを示します。	3
終了した GIOP セッション (GIOP Session Terminated)	18348	GIOP セッションが終了したことを示します。	3
拒否された GIOP セッション (GIOP Session Denied)	18349	GIOP セッションが拒否されたことを示します。	3
進行中の GIOP セッション (GIOP Session In Progress)	18350	GIOP セッションが進行中であることを示します。	1
開かれた Finger セッション (Finger Session Opened)	18351	Finger セッションが確立されたことを示します。	1
閉じられた Finger セッション (Finger Session Closed)	18352	Finger セッションが閉じられたことを示します。	1
リセットされた Finger セッション (Finger Session Reset)	18353	Finger セッションがリセットされたことを示します。	3

表 98. アプリケーション・カテゴリーの下位カテゴリーおよび重大度レベル (続き)

下位イベント・カテゴリー	カテゴリー ID	説明	重大度レベル (0 から 10 まで)
終了した Finger セッション (Finger Session Terminated)	18354	Finger セッションが終了したことを示します。	3
拒否された Finger セッション (Finger Session Denied)	18355	Finger セッションが拒否されたことを示します。	3
進行中の Finger セッション (Finger Session In Progress)	18356	Finger セッションが進行中であることを示します。	1
開かれた Echo セッション (Echo Session Opened)	18357	Echo セッションが確立されたことを示します。	1
閉じられた Echo セッション (Echo Session Closed)	18358	Echo セッションが閉じられたことを示します。	1
拒否された Echo セッション (Echo Session Denied)	18359	Echo セッションが拒否されたことを示します。	3
進行中の Echo セッション (Echo Session In Progress)	18360	Echo セッションが進行中であることを示します。	1
開かれた Remote .NET セッション (Remote .NET Session Opened)	18361	Remote .NET セッションが確立されたことを示します。	1
閉じられた Remote .NET セッション (Remote .NET Session Closed)	18362	Remote .NET セッションが閉じられたことを示します。	1
リセットされた Remote .NET セッション (Remote .NET Session Reset)	18363	Remote .NET セッションがリセットされたことを示します。	3
終了した Remote .NET セッション (Remote .NET Session Terminated)	18364	Remote .NET セッションが終了したことを示します。	3
拒否された Remote .NET セッション (Remote .NET Session Denied)	18365	Remote .NET セッションが拒否されたことを示します。	3
進行中の Remote .NET セッション (Remote .NET Session In Progress)	18366	Remote .NET セッションが進行中であることを示します。	1

表 98. アプリケーション・カテゴリーの下位カテゴリーおよび重大度レベル (続き)

下位イベント・カテゴリー	カテゴリー ID	説明	重大度レベル (0 から 10 まで)
DNP3 セッションのオープン	18367	Distributed Network Proctologic (DNP3) セッションが確立されたことを示します。	1
閉じられた DNP3 セッション (DNP3 Session Closed)	18368	DNP3 セッションが閉じられたことを示します。	1
リセットされた DNP3 セッション (DNP3 Session Reset)	18369	DNP3 セッションがリセットされたことを示します。	3
終了した DNP3 セッション (DNP3 Session Terminated)	18370	DNP3 セッションが終了したことを示します。	3
拒否された DNP3 セッション (DNP3 Session Denied)	18371	DNP3 セッションが拒否されたことを示します。	3
進行中の DNP3 セッション (DNP3 Session In Progress)	18372	DNP3 セッションが進行中であることを示します。	1
開かれた Discard セッション (Discard Session Opened)	18373	Discard セッションが確立されたことを示します。	1
閉じられた Discard セッション (Discard Session Closed)	18374	Discard セッションが閉じられたことを示します。	1
リセットされた Discard セッション (Discard Session Reset)	18375	Discard セッションがリセットされたことを示します。	3
終了した Discard セッション (Discard Session Terminated)	18376	Discard セッションが終了したことを示します。	3
拒否された Discard セッション (Discard Session Denied)	18377	Discard セッションが拒否されたことを示します。	3
進行中の Discard セッション (Discard Session In Progress)	18378	Discard セッションが進行中であることを示します。	1
開かれた DHCP セッション (DHCP Session Opened)	18379	動的ホスト構成プロトコル (DHCP) セッションが確立されたことを示します。	1

表 98. アプリケーション・カテゴリーの下位カテゴリーおよび重大度レベル (続き)

下位イベント・カテゴリー	カテゴリー ID	説明	重大度レベル (0 から 10 まで)
閉じられた DHCP セッション (DHCP Session Closed)	18380	DHCP セッションが閉じられたことを示します。	1
拒否された DHCP セッション (DHCP Session Denied)	18381	DHCP セッションが拒否されたことを示します。	3
進行中の DHCP セッション (DHCP Session In Progress)	18382	DHCP セッションが進行中であることを示します。	1
成功した DHCP (DHCP Success)	18383	DHCP リースが正常に取得されたことを示します	1
失敗した DHCP (DHCP Failure)	18384	DHCP リースが取得できないことを示します。	3
開かれた CVS セッション (CVS Session Opened)	18385	Concurrent Versions System (CVS) セッションが確立されたことを示します。	1
閉じられた CVS セッション (CVS Session Closed)	18386	CVS セッションが閉じられたことを示します。	1
リセットされた CVS セッション (CVS Session Reset)	18387	CVS セッションがリセットされたことを示します。	3
終了した CVS セッション (CVS Session Terminated)	18388	CVS セッションが終了したことを示します。	3
拒否された CVS セッション (CVS Session Denied)	18389	CVS セッションが拒否されたことを示します。	3
進行中の CVS セッション (CVS Session In Progress)	18390	CVS セッションが進行中であることを示します。	1
開かれた CUPS セッション (CUPS Session Opened)	18391	Common UNIX Printing System (CUPS) セッションが確立されたことを示します。	1
閉じられた CUPS セッション (CUPS Session Closed)	18392	CUPS セッションが閉じられたことを示します。	1

表 98. アプリケーション・カテゴリーの下位カテゴリーおよび重大度レベル (続き)

下位イベント・カテゴリー	カテゴリー ID	説明	重大度レベル (0 から 10 まで)
リセットされた CUPS セッション (CUPS Session Reset)	18393	CUPS セッションがリセットされたことを示します。	3
終了した CUPS セッション (CUPS Session Terminated)	18394	CUPS セッションが終了したことを示します。	3
拒否された CUPS セッション (CUPS Session Denied)	18395	CUPS セッションが拒否されたことを示します。	3
進行中の CUPS セッション (CUPS Session In Progress)	18396	CUPS セッションが進行中であることを示します。	1
開始された Chargen セッション (Chargen Session Started)	18397	Character Generator (Chargen) セッションが開始されたことを示します。	1
閉じられた Chargen セッション (Chargen Session Closed)	18398	Chargen セッションが閉じられたことを示します。	1
リセットされた Chargen セッション (Chargen Session Reset)	18399	Chargen セッションがリセットされたことを示します。	3
終了した Chargen セッション (Chargen Session Terminated)	18400	Chargen セッションが終了したことを示します。	3
拒否された Chargen セッション (Chargen Session Denied)	18401	Chargen セッションが拒否されたことを示します。	3
進行中の Chargen セッション (Chargen Session In Progress)	18402	Chargen セッションが進行中であることを示します。	1
その他の VPN (Misc VPN)	18403	その他の VPN セッションが検出されたことを示します	1
開始された DAP セッション (DAP Session Started)	18404	DAP セッションが確立されたことを示します。	1
終了した DAP セッション (DAP Session Ended)	18405	DAP セッションが終了したことを示します。	1
拒否された DAP セッション (DAP Session Denied)	18406	DAP セッションが拒否されたことを示します。	3

表 98. アプリケーション・カテゴリーの下位カテゴリーおよび重大度レベル (続き)

下位イベント・カテゴリー	カテゴリー ID	説明	重大度レベル (0 から 10 まで)
DAP セッション状況 (DAP Session Status)	18407	DAP セッション状況要求が行われたことを示します。	1
進行中の DAP セッション (DAP Session in Progress)	18408	DAP セッションが進行中であることを示します。	1
失敗した DAP 認証 (DAP Authentication Failed)	18409	DAP 認証が失敗したことを示します。	4
成功した DAP 認証 (DAP Authentication Succeeded)	18410	DAP 認証が成功したことを示します。	1
開始された TOR セッション (TOR Session Started)	18411	TOR セッションが確立されたことを示します。	1
閉じられた TOR セッション (TOR Session Closed)	18412	TOR セッションが閉じられたことを示します。	1
リセットされた TOR セッション (TOR Session Reset)	18413	TOR セッションがリセットされたことを示します。	3
終了した TOR セッション (TOR Session Terminated)	18414	TOR セッションが終了したことを示します。	3
拒否された TOR セッション (TOR Session Denied)	18415	TOR セッションが拒否されたことを示します。	3
進行中の TOR セッション (TOR Session In Progress)	18416	TOR セッションが進行中であることを示します。	1
開始されたゲーム・セッション (Game Session Started)	18417	ゲーム・セッションが開始されたことを示します。	1
閉じられたゲーム・セッション (Game Session Closed)	18418	ゲーム・セッションが閉じられたことを示します。	1
リセットされたゲーム・セッション (Game Session Reset)	18419	ゲーム・セッションがリセットされたことを示します。	3
終了したゲーム・セッション (Game Session Terminated)	18420	ゲーム・セッションが終了したことを示します。	3

表 98. アプリケーション・カテゴリーの下位カテゴリーおよび重大度レベル (続き)

下位イベント・カテゴリー	カテゴリー ID	説明	重大度レベル (0 から 10 まで)
拒否されたゲーム・セッション (Game Session Denied)	18421	ゲーム・セッションが拒否されたことを示します。	3
進行中のゲーム・セッション (Game Session In Progress)	18422	ゲーム・セッションが進行中であることを示します。	1
管理者ログイン試行 (Admin Login Attempt)	18423	管理ユーザーとしてのログイン試行が検出されたことを示します。	2
ユーザー・ログイン試行 (User Login Attempt)	18424	非管理ユーザーとしてのログイン試行が検出されたことを示します。	2
クライアント・サーバー (Client Server)	18425	クライアント/サーバー・アクティビティーを示します。	1
コンテンツ配信 (Content Delivery)	18426	コンテンツ配信アクティビティーを示します。	1
データ転送 (Data Transfer)	18427	データ転送を示します。	3
データウェアハウジング (Data Warehousing)	18428	データウェアハウジング・アクティビティーを示します。	3
ディレクトリー・サービス (Directory Services)	18429	ディレクトリー・サービス・アクティビティーを示します。	2
ファイル印刷 (File Print)	18430	ファイル印刷アクティビティーを示します。	1
ファイル転送 (File Transfer)	18431	ファイル転送を示します。	2
ゲーム (Games)	18432	ゲーム・アクティビティーを示します。	4
ヘルスケア (Healthcare)	18433	ヘルスケア・アクティビティーを示します。	1
内部システム (Inner System)	18434	内部システム・アクティビティーを示します。	1
インターネット・プロトコル (Internet Protocol)	18435	インターネット・プロトコル・アクティビティーを示します。	1

表 98. アプリケーション・カテゴリーの下位カテゴリーおよび重大度レベル (続き)

下位イベント・カテゴリー	カテゴリー ID	説明	重大度レベル (0 から 10 まで)
レガシー (Legacy)	18436	レガシー・アクティビティーを示します。	1
メール (Mail)	18437	メール・アクティビティーを示します。	1
その他 (Misc)	18438	その他のアクティビティーを示します。	2
マルチメディア (Multimedia)	18439	マルチメディア・アクティビティーを示します。	2
ネットワーク管理	18440	ネットワーク管理アクティビティーを示します。	
P2P	18441	対等通信 (P2P) アクティビティーを示します。	4
リモート・アクセス (Remote Access)	18442	リモート・アクセス・アクティビティーを示します。	3
ルーティング・プロトコル (Routing Protocols)	18443	ルーティング・プロトコル・アクティビティーを示します。	1
セキュリティー・プロトコル (Security Protocols)	18444	セキュリティー・プロトコル・アクティビティーを示します。	2
ストリーミング (Streaming)	18445	ストリーミング・アクティビティーを示します。	2
通常ではないプロトコル (Uncommon Protocol)	18446	通常ではないプロトコル・アクティビティーを示します。	3
VoIP	18447	VoIP アクティビティーを示します。	1
Web	18448	Web アクティビティーを示します。	1
ICMP	18449	ICMP アクティビティーを示します。	1

監査

監査カテゴリーには、E メール・アクティビティーや FTP アクティビティーなどの、監査アクティビティーに関連するイベントが含まれます。

以下の表で、監査カテゴリーの下位イベント・カテゴリーおよび関連する重大度レベルについて説明します。

表 *99.* 監査カテゴリーの下位カテゴリーおよび重大度レベル

下位イベント・カテゴリー	カテゴリー **ID**	説明	重大度レベル **(0** から **10** まで**)**
一般監査イベント (General Audit Event)	19001	一般監査イベントが開始されたことを示します。	1
組み込み実行 (Built-in Execution)	19002	組み込み監査タスクが実行されたことを示します。	1
一括コピー	19003	データの一括コピーが検出されたことを示します。	1
データ・ダンプ (Data Dump)	19004	データ・ダンプが検出されたことを示します。	1
データのインポート (Data Import)	19005	データのインポートが検出されたことを示します。	1
データ選択 (Data Selection)	19006	データ選択プロセスが検出されたことを示します。	1
データ切り捨て (Data Truncation)	19007	データ切り捨てプロセスが検出されたことを示します。	1
データ更新 (Data Update)	19008	データ更新プロセスが検出されたことを示します。	1
プロシージャー/トリガーの実行 (Procedure/Trigger Execution)	19009	データベースのプロシージャーまたはトリガーの実行が検出されたことを示します。	1
スキーマ変更 (Schema Change)	19010	プロシージャーまたはトリガーを実行するスキーマが変更されたことを示します。	1
作成アクティビティーが試行されました	19011	作成アクティビティーが試行されたことを示します。	1
作成アクティビティーが成功しました	19012	作成アクティビティーが成功したことを示します。	1

表 *99.* 監査カテゴリーの下位カテゴリーおよび重大度レベル (続き)

下位イベント・カテゴリー	カテゴリー **ID**	説明	重大度レベル **(0** から **10** まで**)**
作成アクティビティーが失敗しました	19013	作成アクティビティーが失敗したことを示します。	3
読み取りアクティビティーが試行されました	19014	読み取りアクティビティーが試行されたことを示します。	1
読み取りアクティビティーが成功しました	19015	読み取りアクティビティーが成功したことを示します。	1
読み取りアクティビティーが失敗しました	19016	読み取りアクティビティーが失敗したことを示します。	3
更新アクティビティーが試行されました	19017	更新アクティビティーが試行されたことを示します。	1
更新アクティビティーが成功しました	19018	更新アクティビティーが成功したことを示します。	1
更新アクティビティーが失敗しました	19019	更新アクティビティーが失敗したことを示します。	3
削除アクティビティーが試行されました	19020	削除アクティビティーが試行されたことを示します。	1
削除アクティビティーが成功しました	19021	削除アクティビティーが成功したことを示します。	1
削除アクティビティーが失敗しました	19022	削除アクティビティーが失敗したことを示します。	3
バックアップ・アクティビティーが試行されました	19023	バックアップ・アクティビティーが試行されたことを示します。	1
バックアップ・アクティビティーが成功しました	19024	バックアップ・アクティビティーが成功したことを示します。	1
バックアップ・アクティビティーが失敗しました	19025	バックアップ・アクティビティーが失敗したことを示します。	3

表 99. 監査カテゴリーの下位カテゴリーおよび重大度レベル (続き)

下位イベント・カテゴリー	カテゴリー ID	説明	重大度レベル (0 から 10 まで)
キャプチャー・アクティビティーが試行されました	19026	キャプチャー・アクティビティーが試行されたことを示します。	1
キャプチャー・アクティビティーが成功しました	19027	キャプチャー・アクティビティーが成功したことを示します。	1
キャプチャー・アクティビティーが失敗しました	19028	キャプチャー・アクティビティーが失敗したことを示します。	3
構成アクティビティーが試行されました	19029	構成アクティビティーが試行されたことを示します。	1
構成アクティビティーが成功しました	19030	構成アクティビティーが成功したことを示します。	1
構成アクティビティーが失敗しました	19031	構成アクティビティーが失敗したことを示します。	3
デプロイ・アクティビティーが試行されました	19032	デプロイメント・アクティビティーが試行されたことを示します。	1
デプロイ・アクティビティーが成功しました	19033	デプロイメント・アクティビティーが成功したことを示します。	1
デプロイ・アクティビティーが失敗しました	19034	デプロイメント・アクティビティーが失敗したことを示します。	3
無効化アクティビティーが試行されました	19035	無効化アクティビティーが試行されたことを示します。	1
無効化アクティビティーが成功しました	19036	無効化アクティビティーが成功したことを示します。	1
無効化アクティビティーが失敗しました	19037	無効化アクティビティーが失敗したことを示します。	3
有効化アクティビティーが試行されました	19038	有効化アクティビティーが試行されたことを示します。	1

表 99. 監査カテゴリーの下位カテゴリーおよび重大度レベル (続き)

下位イベント・カテゴリー	カテゴリー **ID**	説明	重大度レベル **(0** から **10** まで**)**
有効化アクティビティーが成功しました	19039	有効化アクティビティーが成功したことを示します。	1
有効化アクティビティーが失敗しました	19040	有効化アクティビティーが失敗したことを示します。	3
モニター・アクティビティーが試行されました	19041	モニター・アクティビティーが試行されたことを示します。	1
モニター・アクティビティーが成功しました	19042	モニター・アクティビティーが成功したことを示します。	1
モニター・アクティビティーが失敗しました	19043	モニター・アクティビティーが失敗したことを示します。	3
リストア・アクティビティーが試行されました	19044	リストア・アクティビティーが試行されたことを示します。	1
リストア・アクティビティーが成功しました	19045	リストア・アクティビティーが成功したことを示します。	1
リストア・アクティビティーが失敗しました	19046	リストア・アクティビティーが失敗したことを示します。	3
開始アクティビティーが試行されました	19047	開始アクティビティーが試行されたことを示します。	1
開始アクティビティーが成功しました	19048	開始アクティビティーが成功したことを示します。	1
開始アクティビティーが失敗しました	19049	開始アクティビティーが失敗したことを示します。	3
停止アクティビティーが試行されました	19050	停止アクティビティーが試行されたことを示します。	1
停止アクティビティーが成功しました	19051	停止アクティビティーが成功したことを示します。	1
停止アクティビティーが失敗しました	19052	停止アクティビティーが失敗したことを示します。	3

表 *99.* 監査カテゴリーの下位カテゴリーおよび重大度レベル (続き)

下位イベント・カテゴリー	カテゴリー **ID**	説明	重大度レベル **(0** から **10** まで**)**
アンデプロイ・アクティビティーが試行されました	19053	アンデプロイ・アクティビティーが試行されたことを示します。	1
アンデプロイ・アクティビティーが成功しました	19054	アンデプロイ・アクティビティーが成功したことを示します。	1
アンデプロイ・アクティビティーが失敗しました	19055	アンデプロイ・アクティビティーが失敗したことを示します。	3
受信アクティビティーが試行されました	19056	受信アクティビティーが試行されたことを示します。	1
受信アクティビティーが成功しました	19057	受信アクティビティーが成功したことを示します。	1
受信アクティビティーが失敗しました	19058	受信アクティビティーが失敗したことを示します。	3
送信アクティビティーが試行されました	19059	送信アクティビティーが試行されたことを示します。	1
送信アクティビティーが成功しました	19060	送信アクティビティーが成功したことを示します。	1
送信アクティビティーが失敗しました	19061	送信アクティビティーが失敗したことを示します。	3

リスク

リスク・カテゴリーには、IBM Security QRadar Risk Manager に関連するイベントが含まれます。

以下の表で、リスク・カテゴリーの下位イベント・カテゴリーとそれに関連する重大度レベルについて説明します。

表 *100.* リスク・カテゴリーの下位イベント・カテゴリーと重大度レベル

下位イベント・カテゴリー	カテゴリー **ID**	説明	重大度レベル **(0** から **10** まで**)**
ポリシー公開	20001	ポリシーの露出が検出されたことを示します。	5

表 *100.* リスク・カテゴリーの下位イベント・カテゴリーと重大度レベル *(*続き*)*

下位イベント・カテゴリー	カテゴリー **ID**	説明	重大度レベル **(0** から **10** まで**)**
コンプライアンス違反 (Compliance Violation)	20002	コンプライアンス違反が検出されたことを示します。	5
露出した脆弱性 (Exposed Vulnerability)	20003	ネットワークまたはデバイスには露出した脆弱性があることを示します。	9
リモート・アクセスの脆弱性 (Remote Access Vulnerability)	20004	ネットワークまたはデバイスにはリモート・アクセスの脆弱性があることを示します。	9
ローカル・アクセスの脆弱性 (Local Access Vulnerability)	20005	ネットワークまたはデバイスにはローカル・アクセスの脆弱性があることを示します。	7
無線のオープン・アクセス (Open Wireless Access)	20006	ネットワークまたはデバイスには無線のオープン・アクセスがあることを示します。	5
弱い暗号化 (Weak Encryption)	20007	ホストまたはデバイスには弱い暗号化があることを示します。	5
暗号化されていないデータ転送 (Un-Encrypted Data Transfer)	20008	暗号化されていないデータをホストまたはデバイスが転送していることを示します。	3
暗号化されていないデータ・ストア (Un-Encrypted Data Store)	20009	データ・ストアが暗号化されていないことを示します。	3
誤った構成のルール (Mis-Configured Rule)	20010	ルールが正しく構成されていないことを示します。	3
誤った構成のデバイス (Mis-Configured Device)	20011	ネットワーク上のデバイスが正しく構成されていないことを示します。	3

表 *100.* リスク・カテゴリーの下位イベント・カテゴリーと重大度レベル (続き)

下位イベント・カテゴリー	カテゴリー **ID**	説明	重大度レベル **(0** から **10** まで**)**
誤った構成のホスト (Mis-Configured Host)	20012	ネットワーク・ホストが正しく構成されていないことを示します。	3
データ損失の可能性 (Data Loss Possible)	20013	データ損失の可能性が検出されたことを示します。	5
弱い認証 (Weak Authentication)	20014	ホストまたはデバイスが不正行為を受けやすいことを示します。	5
パスワードなし (No Password)	20015	パスワードが存在しないことを示します。	7
不正行為 (Fraud)	20016	ホストまたはデバイスが不正行為を受けやすいことを示します。	7
DoS ターゲットの可能性 (Possible DoS Target)	20017	ホストまたはデバイスは DoS ターゲットの可能性があることを示します。	3
DoS 脆弱性の可能性 (Possible DoS Weakness)	20018	ホストまたはデバイスに DoS 脆弱性の可能性があることを示します。	3
機密性の消失 (Loss of Confidentiality)	20019	機密性の消失が検出されたことを示します。	5
ポリシー・モニターのリスク・スコア集計 (Policy Monitor Risk Score Accumulation)	20020	ポリシー・モニターのリスク・スコア集計が検出されたことを示します。	1

リスク・マネージャー監査

リスク・マネージャー監査カテゴリーには、IBM Security QRadar Risk Manager の監査イベントに関連するイベントが含まれます。

以下の表で、リスク・マネージャー監査カテゴリーの下位イベント・カテゴリーとそれに関連する重大度レベルについて説明します。

表 *101.* リスク・マネージャー監査カテゴリーの下位イベント・カテゴリーと重大度レベル

下位イベント・カテゴリー	カテゴリー **ID**	説明	重大度レベル **(0** から **10** まで**)**
ポリシー・モニター	21001	ポリシー・モニターが変更されたことを示します。	3
トポロジー	21002	トポロジーが変更されたことを示します。	3
シミュレーション	21003	シミュレーションが変更されたことを示します。	3
管理	21004	管理変更が行われたことを示します。	3

制御

制御カテゴリーには、ハードウェア・システムに関連したイベントが含まれます。

以下の表で、制御カテゴリーの下位イベント・カテゴリーおよび関連する重大度レベルについて説明します。

表 *102.* 制御カテゴリーの下位カテゴリーおよび重大度レベル

下位イベント・カテゴリー	カテゴリー **ID**	説明	重大度レベル **(0** から **10** まで**)**
読み取られたデバイス (Device Read)	22001	デバイスが読み取られたことを示します。	1
デバイス通信 (Device Communication)	22002	デバイスとの通信を示します。	1
デバイス監査 (Device Audit)	22003	デバイス監査が行われたことを示します。	1
デバイス・イベント (Device Event)	22004	デバイス・イベントが発生したことを示します。	1
デバイス ping (Device Ping)	22005	デバイスへの ping アクションが発生したことを示します。	1
デバイス構成 (Device Configuration)	22006	デバイスが構成したことを示します。	1
デバイスの登録	22007	デバイスが登録されたことを示します。	1

表 *102.* 制御カテゴリーの下位カテゴリーおよび重大度レベル *(*続き*)*

下位イベント・カテゴリー	カテゴリー **ID**	説明	重大度レベル **(0** から **10** まで**)**
デバイス・ルート (Device Route)	22008	デバイス・ルート・アクションが発生したことを示します。	1
デバイス・インポート (Device Import)	22009	デバイス・インポートが発生したことを示します。	1
デバイス情報 (Device Information)	22010	デバイス情報アクションが発生したことを示します。	1
デバイス警告 (Device Warning)	22011	デバイスに対して警告が生成されたことを示します。	1
デバイス・エラー (Device Error)	22012	デバイスに対してエラーが生成されたことを示します。	1
リレー・イベント (Relay Event)	22013	リレー・イベントを示します。	1
NIC イベント (NIC Event)	22014	ネットワーク・インターフェース・カード (NIC) イベントを示します。	1
UIQ イベント	22015	モバイル・デバイスのイベントを示します。	1
IMU イベント (IMU Event)	22016	Integrated Management Unit (IMU) のイベントを示します。	1
請求イベント (Billing Event)	22017	請求イベントを示します。	1
DBMS イベント (DBMS Event)	22018	データベース管理システム (DBMS) のイベントを示します。	1
インポート・イベント (Import Event)	22019	インポートが行われたことを示します。	1
ロケーション・インポート (Location Import)	22020	ロケーション・インポートが行われたことを示します。	1
ルート・インポート (Route Import)	22021	ルート・インポートが行われたことを示します。	1
エクスポート・イベント (Export Event)	22022	エクスポートが行われたことを示します。	1

表 *102.* 制御カテゴリーの下位カテゴリーおよび重大度レベル (続き)

下位イベント・カテゴリー	カテゴリー **ID**	説明	重大度レベル **(0** から **10** まで**)**
リモート信号 (Remote Signaling)	22023	リモート信号を示します。	1
ゲートウェイ状況 (Gateway Status)	22024	ゲートウェイ状況を示します。	1
ジョブ・イベント (Job Event)	22025	ジョブが発生したことを示します。	1
セキュリティー・イベント (Security Event)	22026	セキュリティー・イベントが発生したことを示します。	1
デバイス改ざん検出 (Device Tamper Detection)	22027	システムが改ざん行為を検出したことを示します。	1
時間イベント (Time Event)	22028	時間イベントが発生したことを示します。	1
疑わしい振る舞い	22029	疑わしい振る舞いが発生したことを示します。	1
停電 (Power Outage)	22030	停電が発生したことを示します。	1
電力回復 (Power Restoration)	22031	電力が回復したことを示します。	1
ハートビート (Heartbeat)	22032	ハートビート ping が発生したことを示します。	1
リモート接続イベント (Remote Connection Event)	22033	システムへのリモート接続を示します。	1

アセット・プロファイラー

アセット・プロファイラー・カテゴリーには、アセット・プロファイルに関連するイベントが含まれます。

以下の表で、アセット・プロファイラー・カテゴリーの下位イベント・カテゴリーおよび関連する重大度レベルを説明します。

表 *103.* アセット・プロファイラー・カテゴリーの下位カテゴリーおよび重大度レベル

下位イベント・カテゴリー	カテゴリー **ID**	説明	重大度レベル **(0** から **10** まで**)**
作成されたアセット (Asset Created)	23001	アセットが作成されたことを示します。	1
更新されたアセット (Asset Updated)	23002	アセットが更新されたことを示します。	1

表 *103.* アセット・プロファイラー・カテゴリーの下位カテゴリーおよび重大度レベル *(*続き*)*

下位イベント・カテゴリー	カテゴリー **ID**	説明	重大度レベル **(0** から **10** まで**)**
監視されたアセット (Asset Observed)	23003	アセットが監視されたことを示します。	1
移動されたアセット (Asset Moved)	23004	アセットが移動されたことを示します。	1
削除されたアセット (Asset Deleted)	23005	アセットが削除されたことを示します。	1
クリーンされたアセット・ホスト名 (Asset Hostname Cleaned)	23006	ホスト名がクリーンされたことを示します。	1
作成されたアセット・ホスト名 (Asset Hostname Created)	23007	ホスト名が作成されたことを示します。	1
更新されたアセット・ホスト名 (Asset Hostname Updated)	23008	ホスト名が更新されたことを示します。	1
監視されたアセット・ホスト名 (Asset Hostname Observed)	23009	ホスト名が監視されたことを示します。	1
移動されたアセット・ホスト名 (Asset Hostname Moved)	23010	ホスト名が移動されたことを示します。	1
削除されたアセット・ホスト名 (Asset Hostname Deleted)	23011	ホスト名が削除されたことを示します。	1
クリーンされたアセット・ポート (Asset Port Cleaned)	23012	ポートがクリーンされたことを示します。	1
作成されたアセット・ポート (Asset Port Created)	23013	ポートが作成されたことを示します。	1
更新されたアセット・ポート (Asset Port Updated)	23014	ポートが更新されたことを示します。	1
監視されたアセット・ポート (Asset Port Observed)	23015	ポートが監視されたことを示します。	1
移動されたアセット・ポート (Asset Port Moved)	23016	ポートが移動されたことを示します。	1
削除されたアセット・ポート (Asset Port Deleted)	23017	ポートが削除されたことを示します。	1

表 *103.* アセット・プロファイラー・カテゴリーの下位カテゴリーおよび重大度レベル *(*続き*)*

下位イベント・カテゴリー	カテゴリー **ID**	説明	重大度レベル **(0** から **10** まで**)**
クリーンされたアセット脆弱性インスタンス (Asset Vuln Instance Cleaned)	23018	脆弱性インスタンスがクリーンされたことを示します。	1
作成されたアセット脆弱性インスタンス (Asset Vuln Instance Created)	23019	脆弱性インスタンスが作成されたことを示します。	1
更新されたアセット脆弱性インスタンス (Asset Vuln Instance Updated)	23020	脆弱性インスタンスが更新されたことを示します。	1
監視されたアセット脆弱性インスタンス (Asset Vuln Instance Observed)	23021	脆弱性インスタンスが監視されたことを示します。	1
移動されたアセット脆弱性インスタンス (Asset Vuln Instance Moved)	23022	脆弱性インスタンスが移動されたことを示します。	1
削除されたアセット脆弱性インスタンス (Asset Vuln Instance Deleted)	23023	脆弱性インスタンスが削除されたことを示します。	1
クリーンされたアセット OS (Asset OS Cleaned)	23024	オペレーティング・システムがクリーンされたことを示します。	1
作成されたアセット OS (Asset OS Created)	23025	オペレーティング・システムが作成されたことを示します。	1
更新されたアセット OS (Asset OS Updated)	23026	オペレーティング・システムが更新されたことを示します。	1
監視されたアセット OS (Asset OS Observed)	23027	オペレーティング・システムが監視されたことを示します。	1
移動されたアセット OS (Asset OS Moved)	23028	オペレーティング・システムが移動されたことを示します。	1
削除されたアセット OS (Asset OS Deleted)	23029	オペレーティング・システムが削除されたことを示します。	1

表 *103.* アセット・プロファイラー・カテゴリーの下位カテゴリーおよび重大度レベル *(*続き*)*

下位イベント・カテゴリー	カテゴリー **ID**	説明	重大度レベル **(0** から **10** まで**)**
クリーンされたアセット・プロパティー (Asset Property Cleaned)	23030	プロパティーがクリーンされたことを示します。	1
作成されたアセット・プロパティー (Asset Property Created)	23031	プロパティーが作成されたことを示します。	1
更新されたアセット・プロパティー (Asset Property Updated)	23032	プロパティーが更新されたことを示します。	1
監視されたアセット・プロパティー (Asset Property Observed)	23033	プロパティーが監視されたことを示します。	1
移動されたアセット・プロパティー (Asset Property Moved)	23034	プロパティーが削除されたことを示します。	1
削除されたアセット・プロパティー (Asset Property Deleted)	23035	プロパティーが削除されたことを示します。	1
クリーンされたアセット IP アドレス (Asset IP Address Cleaned)	23036	IP アドレスがクリーンされたことを示します。	1
作成されたアセット IP アドレス (Asset IP Address Created)	23037	IP アドレスが作成されたことを示します。	1
更新されたアセット IP アドレス (Asset IP Address Updated)	23038	IP アドレスが更新されたことを示します。	1
監視されたアセット IP アドレス (Asset IP Address Observed)	23039	IP アドレスが監視されたことを示します。	1
移動されたアセット IP アドレス (Asset IP Address Moved)	23040	IP アドレスが移動されたことを示します。	1

表 *103.* アセット・プロファイラー・カテゴリーの下位カテゴリーおよび重大度レベル *(*続き*)*

下位イベント・カテゴリー	カテゴリー **ID**	説明	重大度レベル **(0** から **10** まで**)**
削除されたアセット IP アドレス (Asset IP Address Deleted)	23041	IP アドレスが削除されたことを示します。	1
クリーンされたアセット・インターフェース (Asset Interface Cleaned)	23042	インターフェースがクリーンされたことを示します。	1
作成されたアセット・インターフェース (Asset Interface Created)	23043	インターフェースが作成されたことを示します。	1
アセット・インターフェース更新	23044	インターフェースが更新されたことを示します。	1
監視されたアセット・インターフェース (Asset Interface Observed)	23045	インターフェースが監視されたことを示します。	1
移動されたアセット・インターフェース (Asset Interface Moved)	23046	インターフェースが移動されたことを示します。	1
マージされたアセット・インターフェース (Asset Interface Merged)	23047	インターフェースがマージされたことを示します。	1
アセット・インターフェース削除	23048	インターフェースが削除されたことを示します。	1
クリーンされたアセット・ユーザー (Asset User Cleaned)	23049	ユーザーがクリーンされたことを示します。	1
監視されたアセット・ユーザー (Asset User Observed)	23050	ユーザーが監視されたことを示します。	1
移動されたアセット・ユーザー (Asset User Moved)	23051	ユーザーが移動されたことを示します。	1
削除されたアセット・ユーザー (Asset User Deleted)	23052	ユーザーが削除されたことを示します。	1

表 *103.* アセット・プロファイラー・カテゴリーの下位カテゴリーおよび重大度レベル *(*続き*)*

下位イベント・カテゴリー	カテゴリー **ID**	説明	重大度レベル **(0** から **10** まで**)**
クリーンされたアセット・スキャン・ポリシー (Asset Scanned Policy Cleaned)	23053	スキャン・ポリシーがクリーンされたことを示します。	1
監視されたアセット・スキャン・ポリシー (Asset Scanned Policy Observed)	23054	スキャン・ポリシーが監視されたことを示します。	1
移動されたアセット・スキャン・ポリシー (Asset Scanned Policy Moved)	23055	スキャン・ポリシーが移動されたことを示します。	1
削除されたアセット・スキャン・ポリシー (Asset Scanned Policy Deleted)	23056	スキャン・ポリシーが削除されたことを示します。	1
クリーンされたアセット Windows アプリケーション (Asset Windows Application Cleaned)	23057	Windows アプリケーションがクリーンされたことを示します。	1
監視されたアセット Windows アプリケーション (Asset Windows Application Observed)	23058	Windows アプリケーションが監視されたことを示します。	1
移動されたアセット Windows アプリケーション (Asset Windows Application Moved)	23059	Windows アプリケーションが移動されたことを示します。	1
削除されたアセット Windows アプリケーション (Asset Windows Application Deleted)	23060	Windows アプリケーションが削除されたことを示します。	1
クリーンされたアセット・スキャン・サービス (Asset Scanned Service Cleaned)	23061	スキャン・サービスがクリーンされたことを示します。	1

表 *103.* アセット・プロファイラー・カテゴリーの下位カテゴリーおよび重大度レベル *(*続き*)*

下位イベント・カテゴリー	カテゴリー **ID**	説明	重大度レベル **(0** から **10** まで**)**
監視されたアセット・スキャン・サービス (Asset Scanned Service Observed)	23062	スキャン・サービスが監視されたことを示します。	1
移動されたアセット・スキャン・サービス (Asset Scanned Service Moved)	23063	スキャン・サービスが移動されたことを示します。	1
削除されたアセット・スキャン・サービス (Asset Scanned Service Deleted)	23064	スキャン・サービスが削除されたことを示します。	1
クリーンされたアセット Windows パッチ (Asset Windows Patch Cleaned)	23065	Windows パッチがクリーンされたことを示します。	1
監視されたアセット Windows パッチ (Asset Windows Patch Observed)	23066	Windows パッチが監視されたことを示します。	1
移動されたアセット Windows パッチ (Asset Windows Patch Moved)	23067	Windows パッチが移動されたことを示します。	1
削除されたアセット Windows パッチ (Asset Windows Patch Deleted)	23068	Windows パッチが削除されたことを示します。	1
クリーンされたアセット UNIX パッチ (Asset UNIX Patch Cleaned)	23069	UNIX パッチがクリーンされたことを示します。	1
監視されたアセット UNIX パッチ (Asset UNIX Patch Observed)	23070	UNIX パッチが監視されたことを示します。	1
移動されたアセット UNIX パッチ (Asset UNIX Patch Moved)	23071	UNIX パッチが移動されたことを示します。	1
削除されたアセット UNIX パッチ (Asset UNIX Patch Deleted)	23072	UNIX パッチが削除されたことを示します。	1

表 *103.* アセット・プロファイラー・カテゴリーの下位カテゴリーおよび重大度レベル *(*続き*)*

下位イベント・カテゴリー	カテゴリー **ID**	説明	重大度レベル **(0** から **10** まで**)**
クリーンされたアセット・パッチ・スキャン (Asset Patch Scan Cleaned)	23073	パッチ・スキャンがクリーンされたことを示します。	1
作成されたアセット・パッチ・スキャン (Asset Patch Scan Created)	23074	パッチ・スキャンが作成されたことを示します。	1
アセット・パッチ・スキャンの移動	23075	ポート・スキャンが移動されたことを示します。	1
削除されたアセット・パッチ・スキャン (Asset Patch Scan Deleted)	23076	ポート・スキャンが削除されたことを示します。	1
クリーンされたアセット・ポート・スキャン (Asset Port Scan Cleaned)	23077	ポート・スキャンが作成されたことを示します。	1
アセット・ポート・スキャンの作成	23078	ポート・スキャンが作成されたことを示します。	1
移動されたアセット・ポート・スキャン (Asset Port Scan Moved)	23079	ポート・スキャンが移動されたことを示します。	1
削除されたアセット・ポート・スキャン (Asset Port Scan Deleted)	23080	ポート・スキャンが削除されたことを示します。	1
クリーンされたアセット・クライアント・アプリケーション (Asset Client Application Cleaned)	23081	クライアント・アプリケーションがクリーンされたことを示します。	1
監視されたアセット・クライアント・アプリケーション (Asset Client Application Observed)	23082	クライアント・アプリケーションが監視されたことを示します。	1

表 *103.* アセット・プロファイラー・カテゴリーの下位カテゴリーおよび重大度レベル *(*続き*)*

下位イベント・カテゴリー	カテゴリー **ID**	説明	重大度レベル **(0** から **10** まで**)**
移動されたアセット・クライアント・アプリケーション (Asset Client Application Moved)	23083	クライアント・アプリケーションが移動されたことを示します。	1
削除されたアセット・クライアント・アプリケーション (Asset Client Application Deleted)	23084	クライアント・アプリケーションが削除されたことを示します。	1
監視されたアセット・パッチ・スキャン (Asset Patch Scan Observed)	23085	パッチ・スキャンが監視されたことを示します。	1
監視されたアセット・ポート・スキャン (Asset Port Scan Observed)	23086	ポート・スキャンが監視されたことを示します。	1
NetBIOS グループの作成	23087	NetBIOS グループが作成されたことを示します。	1
NetBIOS グループの更新	23088	NetBIOS グループが更新されたことを示します。	1
NetBIOS グループの監視	23089	NetBIOS グループが監視されたことを示します。	1
NetBIOS グループの削除	23090	NetBIOS グループが削除されたことを示します。	1
NetBIOS グループのクリーンアップ	23091	NetBIOS グループがクリーンアップされたことを示します。	1
NetBIOS グループの移動	23092	NetBIOS グループが移動されたことを示します。	1

センス

センス・カテゴリーには、センス・ユーザー動作分析に関連するイベントが含まれます。

以下の表で、センス・カテゴリーの下位イベント・カテゴリーおよび関連する重大度レベルについて説明します。

表 *104.*

下位イベント・カテゴリー	カテゴリー **ID**	説明	重大度レベル **(0** から **10** まで**)**
ユーザー動作	24001	ユーザーの動作を示します。	5
ユーザー地域	24002	ユーザーの地域を示します。	5
ユーザー時間	24003	ユーザーの時間を示します。	5
ユーザー・アクセス	24004	ユーザーのアクセスを示します。	5
ユーザー特権	24005	ユーザーの特権を示します。	5
ユーザー・リスク	24006	ユーザーのリスクを示します。	5
センス・オフェンス	24007	センス・オフェンスが発生したことを示します。	5
リソース・リスク	24008	リスクのあるリソースを示します。	5

第 26 章 QRadar で使用される共通ポートとサーバー

IBM Security QRadar では、特定のポートが準備されていて、QRadar コンポーネントおよび外部インフラストラクチャーから情報を受信できる必要があります。QRadar に最新のセキュリティー情報を確実に使用させるには、パブリック・サーバーおよび RSS フィードにアクセスする必要もあります。

ポート 22 での SSH 通信

QRadar コンソールが管理対象ホストとの通信に使用するすべてのポートは、暗号化することにより、SSH 経由でポート 22 をトンネリングできます。

コンソールは、安全に通信するために、暗号化された SSH セッションを使用して管理対象ホストに接続します。SSH セッションは、コンソールから開始されて、管理対象ホストにデータを提供します。例えば、QRadar コンソールは、安全に通信するために、イベント・プロセッサーのアプライアンスに対して複数のSSH セッションを開始することができます。この通信では、SSH 経由でトンネリングされたポートが使用される場合があります (HTTPS データの場合はポート 443、Ariel の照会データの場合はポート 32006 など)。暗号化を使用する IBM Security QRadar QFlow Collectorは、データを必要とするフロー・プロセッサーのアプライアンスに対して SSH セッションを開始することができます。

QRadar で必要とされない開いているポート

以下の状態では、追加の開かれているポートが検出される場合があります。

- 所有ハードウェアに QRadar をインストールすると、Red Hat Enterprise Linux に含まれるサービス、デーモン、およびプログラムによって使用されるポートが開かれる場合があります。
- ネットワーク・ファイル共有をマウントまたはエクスポートすると、RPC サービス (`rpc.mountd`、`rpc.rquotad` など) が必要とするポートが動的に割り当てられる場合があります。

関連概念:

5 ページの『IBM Security QRadar 製品の機能』

IBM Security QRadar 製品資料では、オフェンス、フロー、アセット、ヒストリカル相関などの機能について説明していますが、すべての QRadar 製品でこれらの機能を利用できるわけではありません。使用する製品によっては、説明されている一部の機能をデプロイメントで使用できない場合があります。各製品の機能を確認して、必要な情報を入手してください。

QRadar でのポートの使用状況

IBM Security QRadar のサービスおよびコンポーネントがネットワークでの通信に使用する共通のポートのリストを示します。このポートのリストを使用すると、ネットワークで開く必要があるポートを判別できます。例えば、QRadar コンソールがリモートのイベント・プロセッサーと通信するために開く必要があるポートを判別できます。

WinCollect リモート・ポーリング

WinCollect エージェントがリモート側から他の Microsoft Windows オペレーティング・システムをポーリングする場合は、追加のポート割り当てが必要になることがあります。

詳しくは、IBM Security QRadar WinCollect の「ユーザー・ガイド」を参照してください。

QRadar の listen ポート

LISTEN 状態で開かれる QRadar ポートを以下の表に示します。LISTEN ポートが有効になるのは、ご使用のシステムで iptables が有効になっている場合のみです。特記しない限り、割り当て済みポート番号に関する情報はすべての QRadar 製品に該当します。

表 *105. QRadar* サービスおよびコンポーネントが使用する *listen* ポート

ポート	説明	プロトコル	方向	要件
22	SSH	TCP	QRadar コンソールから他のすべてのコンポーネントへの双方向通信。	リモート管理アクセス。 リモート・システムを管理対象ホストとして追加。 ログ・ファイル・プロトコルなど、外部デバイスからファイルを取得するためのログ・ソース・プロトコル。 コマンド・ライン・インターフェースを使用してデスクトップからコンソールへの通信を行うユーザー。 高可用性 (HA)。
25	SMTP	TCP	すべての管理対象ホストから SMTP ゲートウェイへの通信。	QRadar から SMTP ゲートウェイへの E メール。 管理用 E メール連絡先に対するエラー E メール・メッセージと警告 E メール・メッセージの配信。
37	RDATE (時刻)	UDP/ TCP	すべてのシステムから QRadar コンソール。 QRadar コンソールから NTP サーバーまたは RDATE サーバー。	QRadar コンソールと管理対象ホストとの間の時間の同期。

表 *105. QRadar* サービスおよびコンポーネントが使用する *listen* ポート *(*続き*)*

ポート	説明	プロトコル	方向	要件
111	ポートマッパー	TCP/UDP	QRadar コンソール と通信する管理対象ホスト。 QRadar コンソールに接続するユーザー。	ネットワーク・ファイル・システム (NFS) などの必須サービス用のリモート・プロシージャー・コール (RPC)。
135 と、RPC 呼び出しの場合に動的に割り当てられる 1024 よりも上のポート番号。	DCOM	TCP	WinCollect エージェントと、リモートでイベントがポーリングされる Windows オペレーティング・システムとの間の双方向トラフィック。 Microsoft セキュリティー・イベント・ログ・プロトコルまたは Adaptive Log Exporter エージェントのいずれかを使用する QRadar コンソール・コンポーネントまたは IBM Security QRadar イベント・コレクターと、リモートでイベントがポーリングされる Windows オペレーティング・システムの間での双方向トラフィック。	このトラフィックは、WinCollect、Microsoft セキュリティー・イベント・ログ・プロトコルまたは Adaptive Log Exporter によって生成されます。 **注:** DCOM は通常、ランダムなポート範囲を通信用に割り振ります。特定のポートを使用するように Microsoft Windows 製品を構成することができます。詳しくは、Microsoft Windows の資料を参照してください。
137	Windows NetBIOS ネーム・サービス	UDP	WinCollect エージェントと、リモートでイベントがポーリングされる Windows オペレーティング・システムとの間の双方向トラフィック。 Microsoft セキュリティー・イベント・ログ・プロトコルまたは Adaptive Log Exporter エージェントのいずれかを使用する QRadar コンソール・コンポーネントまたは QRadar Event Collectorsと、リモートでイベントがポーリングされる Windows オペレーティング・システムの間での双方向トラフィック。	このトラフィックは、WinCollect、Microsoft セキュリティー・イベント・ログ・プロトコルまたは Adaptive Log Exporter によって生成されます。

表 *105. QRadar* サービスおよびコンポーネントが使用する *listen* ポート *(*続き*)*

ポート	説明	プロトコル	方向	要件
138	Windows NetBIOS データグラム・サービス	UDP	WinCollect エージェントと、リモートでイベントがポーリングされる Windows オペレーティング・システムとの間の双方向トラフィック。 Microsoft セキュリティー・イベント・ログ・プロトコルまたは Adaptive Log Exporter エージェントのいずれかを使用する QRadar コンソール・コンポーネントまたは QRadar Event Collectorsと、リモートでイベントがポーリングされる Windows オペレーティング・システムの間での双方向トラフィック。	このトラフィックは、WinCollect、Microsoft セキュリティー・イベント・ログ・プロトコルまたは Adaptive Log Exporter によって生成されます。
139	Windows NetBIOS セッション・サービス	TCP	WinCollect エージェントと、リモートでイベントがポーリングされる Windows オペレーティング・システムとの間の双方向トラフィック。 Microsoft セキュリティー・イベント・ログ・プロトコルまたは Adaptive Log Exporter エージェントのいずれかを使用する QRadar コンソール・コンポーネントまたは QRadar Event Collectorsと、リモートでイベントがポーリングされる Windows オペレーティング・システムの間での双方向トラフィック。	このトラフィックは、WinCollect、Microsoft セキュリティー・イベント・ログ・プロトコルまたは Adaptive Log Exporter によって生成されます。
162	NetSNMP	UDP	QRadar コンソールに接続する QRadar の管理対象ホスト。 外部ログ・ソースから QRadar Event Collectors。	外部のログ・ソースからの通信 (v1、v2c、および v3) を listen する NetSNMP デーモン用の UDP ポート。このポートは、SNMP エージェントが有効な場合にのみ開かれます。

表 105. QRadar サービスおよびコンポーネントが使用する listen ポート (続き)

ポート	説明	プロトコル	方向	要件
199	NetSNMP	TCP	QRadar コンソールに接続する QRadar の管理対象ホスト。 外部ログ・ソースから QRadar Event Collectors。	外部のログ・ソースからの通信 (v1、v2c、および v3) を listen する NetSNMP デーモン用の TCP ポート。このポートは、SNMP エージェントが有効な場合にのみ開かれます。
427	Service Location Protocol (SLP)	UDP/TCP		統合管理モジュールは、このポートを使用して LAN 上のサービスを検出します。
443	Apache/HTTPS	TCP	すべての製品から QRadar コンソール へのセキュア通信用の双方向トラフィック。	QRadar コンソールから管理対象ホストへの構成のダウンロード。 QRadar コンソールに接続する QRadar の管理対象ホスト。 QRadar へのログイン・アクセス権限を持つユーザー。 WinCollect エージェントに対する構成の更新の管理と提供を行う QRadar コンソール。
445	Microsoft ディレクトリー・サービス	TCP	WinCollect エージェントと、リモートでイベントがポーリングされる Windows オペレーティング・システムとの間の双方向トラフィック。 Microsoft セキュリティー・イベント・ログ・プロトコルを使用する QRadar コンソール・コンポーネントまたは QRadar Event Collectorsと、リモートでイベントがポーリングされる Windows オペレーティング・システムの間での双方向トラフィック。 Adaptive Log Exporter エージェントと、リモートでイベントがポーリングされる Windows オペレーティング・システムとの間の双方向トラフィック。	このトラフィックは、WinCollect、Microsoft セキュリティー・イベント・ログ・プロトコルまたは Adaptive Log Exporter によって生成されます。

表 *105. QRadar* サービスおよびコンポーネントが使用する *listen* ポート *(*続き*)*

ポート	説明	プロトコル	方向	要件
514	Syslog	UDP/TCP	双方向トラフィックを使用する TCP Syslog イベントを提供する外部のネットワーク・アプライアンス。 単一方向トラフィックを使用する UDP Syslog イベントを提供する外部のネットワーク・アプライアンス。 QRadar ホストから QRadar コンソール への内部 Syslog トラフィック。	QRadar コンポーネントにイベント・データを送信するための外部のログ・ソース。 Syslog トラフィックには、UDP イベントまたは TCP イベントを QRadar に送信できる WinCollect エージェント、イベント・コレクター、および Adaptive Log Exporter エージェントが含まれています。
762	ネットワーク・ファイル・システム (NFS) マウント・デーモン (mountd)	TCP/UDP	QRadar コンソールと NFS サーバーとの接続。	指定された場所にファイル・システムをマウントするための要求を処理するネットワーク・ファイル・システム (NFS) マウント・デーモン。
1514	Syslog-ng	TCP/UDP	ロギング用の syslog-ng デーモンに対するローカルのイベント・コレクター・コンポーネントとローカルのイベント・プロセッサー・コンポーネントとの間の接続。	syslog-ng 用の内部ロギング・ポート。
2049	NFS	TCP	QRadar コンソールと NFS サーバーとの接続。	コンポーネント間でファイルやデータを共有するためのネットワーク・ファイル・システム (NFS) プロトコル。
2055	NetFlow データ	UDP	フロー・ソース (通常はルーター) 上の管理インターフェースから IBM Security QRadar QFlow Collector への通信。	ルーターなどのコンポーネントからの NetFlow データグラム。
2375	Docker コマンド・ポート	TCP	内部通信。このポートを外部から使用することはできません。	QRadar アプリケーション・フレームワーク・リソースを管理するために使用されます。

表 *105. QRadar* サービスおよびコンポーネントが使用する *listen* ポート *(*続き*)*

ポート	説明	プロトコル	方向	要件
3389	リモート・デスクトップ・プロトコル (RDP) および Ethernet over USB が有効	TCP/UDP		Microsoft Windows オペレーティング・システムが RDP および Ethernet over USB をサポートするように構成されている場合は、ユーザーが管理ネットワークを介してサーバーとのセッションを開始できます。これは、RDP のデフォルト・ポート 3389 が開いている必要があることを意味します。
3900	統合管理モジュールのリモート・プレゼンス・ポート	TCP/UDP		このポートを使用して、統合管理モジュールを介して QRadar コンソールと対話します。
4333	リダイレクト・ポート	TCP		このポートは、QRadar のオフェンスの解決におけるアドレス解決プロトコル (ARP) 要求のリダイレクト・ポートとして割り当てられています。
5432	Postgres	TCP	ローカルのデータベース・インスタンスへのアクセスに使用される管理対象ホスト用の通信。	「管理」タブから管理対象ホストをプロビジョニングする場合に必要です。
6514	Syslog	TCP	双方向トラフィックを使用する暗号化された TCP Syslog イベントを提供する外部のネットワーク・アプライアンス。	QRadar コンポーネントに暗号化されたイベント・データを送信するための外部のログ・ソース。
6543	高可用性ハートビート	TCP/UDP	HA クラスター内のセカンダリー・ホストとプライマリー・ホスト間の双方向通信。	ハードウェア障害やネットワーク障害を検出するための、HA クラスター内のセカンダリー・ホストからプライマリー・ホストへのハートビート ping。

表 105. QRadar サービスおよびコンポーネントが使用する listen ポート (続き)

ポート	説明	プロトコル	方向	要件
7676, 7677, および 32000 よりも大きな 4 つのランダムなバインド済みポート。	メッセージング接続 (IMQ)	TCP	管理対象ホスト上のコンポーネント間におけるメッセージ・キューの通信。	管理対象ホスト上のコンポーネント間における通信用のメッセージ・キュー・ブローカー。 **注:** QRadar コンソールから暗号化されていないホストへのこれらのポートへのアクセスを許可する必要があります。 ポート 7676 と 7677 は静的 TCP ポートで、4 つの追加の接続がランダムなポート上で作成されます。ランダム・バインド・ポートの確認方法については、 472 ページの『IMQ ポートの関連付けの表示』を参照してください。
7777, 7778, 7779, 7780, 7781, 7782, 7783, 7788, 7790, 7791, 7792, 7793, 7795, 7799, および 8989。	JMX サーバーのポート	TCP	内部通信。これらのポートを外部から使用することはできません。	サポート性能メトリックを公開するための、すべての内部 QRadar プロセスをモニターする JMX サーバー (Java Management Beans)。 これらのポートは、QRadar のサポートで使用されます。
7789	HA Distributed Replicated Block Device	TCP/UDP	HA クラスター内のセカンダリー・ホストとプライマリー・ホスト間の双方向通信。	Distributed Replicated Block Device は、HA 構成におけるプライマリー・ホストとセカンダリー・ホストとの間でドライブの同期を保つために使用されます。
7800	Apache Tomcat	TCP	イベント・コレクターから QRadar コンソール。	イベント用のリアルタイム処理 (ストリーミング)。
7801	Apache Tomcat	TCP	イベント・コレクターから QRadar コンソール。	フロー用のリアルタイム処理 (ストリーミング)。
7803	Apache Tomcat	TCP	イベント・コレクターから QRadar コンソール。	アノマリ検出エンジンのポート。

表 *105. QRadar* サービスおよびコンポーネントが使用する *listen* ポート *(*続き*)*

ポート	説明	プロトコル	方向	要件
7804	QRM Arc ビルダー	TCP	QRadar プロセスと ARC ビルダーの間の内部制御通信。	このポートは QRadar Risk Manager のためにのみ使用されます。外部から使用することはできません。
8000	イベント収集サービス (ECS)	TCP	イベント・コレクターから QRadar コンソール。	特定のイベント・コレクション・サービス (ECS) 用の listen ポート。
8001	SNMP デーモンのポート	UDP	QRadar コンソールからの SNMP トラップ情報を要求する外部の SNMP システム。	外部の SNMP データ要求用の UDP listen ポート。
8005	Apache Tomcat	TCP	内部通信。外部から使用することはできません。	tomcat を制御するために開かれます。 このポートはバインドされており、ローカル・ホストからの接続しか受け入れません。
8009	Apache Tomcat	TCP	HTTP デーモン (HTTPd) プロセスから Tomcat への通信。	Web サービスに対して要求が使用されてプロキシーされる Tomcat コネクター。
8080	Apache Tomcat	TCP	HTTP デーモン (HTTPd) プロセスから Tomcat への通信。	Web サービスに対して要求が使用されてプロキシーされる Tomcat コネクター。
8413	WinCollect エージェント	TCP	WinCollect エージェントと QRadar コンソールの間の双方向トラフィック。	このトラフィックは WinCollect エージェントによって生成され、通信は暗号化されます。構成の更新を WinCollect エージェントに提供し、WinCollect を接続モードで使用する必要があります。
8844	Apache Tomcat	TCP	QRadar コンソールから、QRadar Vulnerability Manager プロセッサーを実行するアプライアンスへの単一方向。	QRadar Vulnerability Manager プロセッサーを実行するホストからの RSS フィードを読み取るために Apache Tomcat によって使用されます。
9090	XForce IP Reputation データベースおよびサーバー	TCP	内部通信。外部から使用することはできません。	QRadar プロセスと XForce Reputation IP データベースの間の通信。

表 *105. QRadar* サービスおよびコンポーネントが使用する *listen* ポート *(*続き*)*

ポート	説明	プロトコル	方向	要件
9913、および 1 つの動的割り当てポート	Web アプリケーション・コンテナー	TCP	Java 仮想マシン間の双方向の Java リモート・メソッド呼び出し (RMI) 通信。	Web アプリケーションが登録されているときは、1 つの追加ポートが動的に割り当てられること。
9995	NetFlow データ	UDP	フロー・ソース (通常はルーター) 上の管理インターフェースから QRadar QFlow コレクター への通信。	ルーターなどのコンポーネントからの NetFlow データグラム。
9999	IBM Security QRadar Vulnerability Manager プロセッサー	TCP	スキャナーから QRadar Vulnerability Manager プロセッサーを実行するアプライアンスまでの単一方向の通信。	QRadar Vulnerability Manager (QVM) コマンド情報のために使用されます。QRadar コンソールは、QRadar Vulnerability Manager プロセッサーを実行するホスト上のこのポートに接続します。このポートは、QVM が有効なときにのみ使用されます。
10000	QRadar Web ベースのシステム管理・インターフェース。	TCP/UDP	ユーザー・デスクトップ・システムからすべての QRadar ホスト。	QRadar V7.2.5 までは、このポートをサーバーの変更 (ホストのルート・パスワードやファイアウォール・アクセスなど) に使用します。 V7.2.6 ではポート 10000 が無効になっています。
10101, 10102	ハートビート・コマンド	TCP	プライマリーおよびセカンダリー HA ノードの間の双方向トラフィック。	HA ノードがアクティブであることを確認するために必要です。
15433	Postgres	TCP	ローカルのデータベース・インスタンスへのアクセスに使用される管理対象ホスト用の通信。	QRadar Vulnerability Manager (QVM) の構成およびストレージに使用されます。このポートは、QVM が有効なときにのみ使用されます。
23111	SOAP Web サーバー	TCP		イベント・コレクション・サービス (ECS) 用の SOAP Web サーバーのポート。
23333	Emulex ファイバー・チャネル	TCP	ファイバー・チャネル・カードを持つ QRadar アプライアンスに接続するユーザー・デスクトップ・システム。	Emulex Fibre Channel HBAnywhere Remote Management サービス (elxmgmt)。

表 *105. QRadar* サービスおよびコンポーネントが使用する *listen* ポート *(*続き*)*

ポート	説明	プロトコル	方向	要件
32004	正規化イベントの転送	TCP	QRadar コンポーネント間の双方向通信。	オフサイト・ソースから、またはQRadar Event Collectors間で転送される正規化イベント・データ。
32005	データ・フロー	TCP	QRadar コンポーネント間の双方向通信。	各イベント・コレクターが個別の管理対象ホスト上に存在する場合の、QRadar Event Collectors間のデータ・フローの通信ポート。
32006	Ariel の照会	TCP	QRadar コンポーネント間の双方向通信。	Ariel プロキシー・サーバーと Ariel 照会サーバー間の通信ポート。
32007	オフェンス・データ	TCP	QRadar コンポーネント間の双方向通信。	オフェンスの一因となっているかグローバル相関に関係するイベントおよびフロー。
32009	アイデンティティー・データ	TCP	QRadar コンポーネント間の双方向通信。	パッシブな脆弱性情報サービス (VIS) とイベント・コレクション・サービス (ECS) との間でやり取りされるアイデンティティー・データ。
32010	フローの listen ソース・ポート	TCP	QRadar コンポーネント間の双方向通信。	QRadar QFlow Collectorからデータを収集するためのフローの listen ポート。
32011	Ariel の listen ポート	TCP	QRadar コンポーネント間の双方向通信。	データベース検索、進行状況情報、およびその他の関連コマンド用の Ariel の listen ポート。
32000-33999	データ・フロー (フロー、イベント、フロー・コンテキスト)	TCP	QRadar コンポーネント間の双方向通信。	各種のデータ・フロー (イベント、フロー、フロー・コンテキスト、イベント検索照会など)。

表 105. *QRadar* サービスおよびコンポーネントが使用する *listen* ポート (続き)

ポート	説明	プロトコル	方向	要件
40799	PCAP データ	UDP	Juniper Networks SRX シリーズのアプライアンスから QRadar への通信。	Juniper Networks SRX シリーズのアプライアンスから着信パケット・キャプチャー (PCAP) データを取得。 **注:** デバイス上のパケット・キャプチャーでは、別のポートを使用することができます。パケット・キャプチャーの構成について詳しくは、Juniper Networks SRX シリーズのアプライアンスの資料を参照してください。
ICMP	ICMP		HA クラスター内のセカンダリー・ホストとプライマリー・ホスト間の双方向トラフィック。	Internet Control Message Protocol (ICMP) を使用して、HA クラスター内のセカンダリー・ホストとプライマリー・ホスト間のネットワーク接続をテストする。

IMQ ポートの関連付けの表示

IBM Security QRadar が使用するいくつかのポートは、ランダムなポート番号を追加で割り振ります。例えば、メッセージ・キュー (IMQ) では、管理対象ホストにあるコンポーネント間の通信のためにランダム・ポートが開かれます。Telnet を使用してローカル・ホストに接続し、ポート番号のルックアップを実行することで、IMQ のランダム・ポート割り当てを確認できます。

ランダム・ポートの関連付けは、静的ポート番号ではありません。サービスが再始動すると、サービスに対して生成されたポートは再割り振りされ、サービスには一連の新しいポート番号が提供されます。

手順

1. SSH を使用して、root ユーザーとして QRadar コンソールにログインします。
2. IMQ メッセージング接続に関連付けられたポートのリストを表示するため、以下のコマンドを入力します。

   `telnet localhost 7676` Telnet コマンドから返される結果は、以下のような出力になります。

```
[root@domain ~]# telnet localhost 7676
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
```

```
101 imqbroker 4.4 Update 1
portmapper tcp PORTMAPPER 7676
[imqvarhome=/opt/openmq/mq/var,imqhome=/opt/openmq/mq,sessionid=<session_id>]
cluster_discovery tcp CLUSTER_DISCOVERY 44913
jmxrmi rmi JMX 0 [url=service:jmx:rmi://domain.ibm.com/stub/<urlpath>]
admin tcp ADMIN 43691
jms tcp NORMAL 7677
cluster tcp CLUSTER 36615
```

Telnet 出力には、IMQ の、ランダムな大きい番号の 4 つの TCP ポートのうちの 3 つが表示されます。表示されない 4 つ目のポートは、出力に示されている JMX URL によって使用可能な JMX リモート・メソッド呼び出し (RMI) ポートです。

Telnet 接続が拒否された場合、IMQ が現在実行されていないことを意味します。おそらく、システムが始動中またはシャットダウン中であるか、サービスが手動でシャットダウンされたものと思われます。

QRadar が使用中のポートの検索

netstat コマンドを使用して、IBM Security QRadar コンソールまたは管理対象ホストで使用中のポートを判別します。**netstat** コマンドを使用して、システム上で listen 中のポートと確立されているポートをすべて表示します。

手順

1. SSH を使用して、root ユーザーとして QRadar コンソールにログインします。
2. アクティブな接続およびコンピューターが listen 中のすべての TCP ポートと UDP ポートを表示するには、以下のコマンドを入力します。

   ```
   netstat -nap
   ```

3. netstat ポートのリストで特定の情報を検索するには、以下のコマンドを入力します。

   ```
   netstat -nap | grep port
   ```

   例:

   - 199 に一致するすべてのポートを表示するには、コマンド

     ```
     netstat -nap | grep 199
     ```

     を入力します。
   - すべての listen 中のポートの情報を表示するには、コマンド

     ```
     netstat -nap | grep LISTEN
     ```

     を入力します。

QRadar パブリック・サーバー

最新のセキュリティー情報を提供するため、IBM Security QRadar は多数のパブリック・サーバーと RSS フィードにアクセスする必要があります。

パブリック・サーバー

表 *106. QRadar* がアクセスする必要があるパブリック・サーバー： 次の表に、QRadar がアクセスする IP アドレスまたはホスト名とその説明を示します。

IP アドレスまたはホスト名	説明
194.153.113.31	IBM Security QRadar Vulnerability Manager DMZ スキャナー
194.153.113.32	QRadar Vulnerability Manager DMZ スキャナー
qmmunity.q1labs.com	QRadar 自動更新サーバー。 自動更新サーバーについて詳しくは、www.ibm.com/support (http://www-01.ibm.com/support/docview.wss?uid=swg21958881) を参照してください。
qmmunity-eu.q1labs.com	QRadar 自動更新サーバー。 自動更新サーバーについて詳しくは、www.ibm.com/support (http://www-01.ibm.com/support/docview.wss?uid=swg21958881) を参照してください。
www.iss.net	IBM Security X-Force Threat Intelligence Threat Information Center ダッシュボード項目
update.xforce-security.com	X-Force Threat Feed 更新サーバー
license.xforce-security.com	X-Force Threat Feed ライセンス・サーバー

QRadar 製品の RSS フィード

表 *107. RSS* フィード： 以下のリストに、QRadar が使用する RSS フィードの要件を説明します。URL をテキスト・エディターにコピーし、改ページを削除してからブラウザーに貼り付けてください。

タイトル	**URL**	要件
Security Intelligence	http://feeds.feedburner.com/SecurityIntelligence	QRadar とインターネット接続
Security Intelligence Vulns / Threats	http://securityintelligence.com/topics/vulnerabilities-threats/feed	QRadar とインターネット接続

表 *107. RSS* フィード *(*続き*)*: 以下のリストに、QRadar が使用する RSS フィードの要件を説明します。URL をテキスト・エディターにコピーし、改ページを削除してからブラウザーに貼り付けてください。

タイトル	**URL**	要件
IBM My Notifications	http://www-945.events.ibm.com/systems/support/myfeed/xmlfeeder.wss?feeder.requid= feeder.create_feed&feeder.feedtype=RSS&feeder.uid=270006EH0R&feeder.subscrid= S14b5f284d32&feeder.subdefkey=swgother&feeder.maxfeed=25	QRadar とインターネット接続
Security News	http://*IP_address_of_QVM_processor* :8844/rss/research/news.rss	IBM Security QRadar Vulnerability Manager プロセッサーがデプロイされていること
Security Advisories	http://*IP_address_of_QVM_processor* :8844/rss/research/advisories.rss	QRadar Vulnerability Manager プロセッサーがデプロイされていること
Latest Published Vulnerabilities	http://*IP_address_of_QVM_processor* :8844/rss/research/vulnerabilities.rss	QRadar Vulnerability Manager プロセッサーがデプロイされていること
Scans Completed	http://*IP_address_of_QVM_processor* :8844/rss/scanresults/completedScans.rss	QRadar Vulnerability Manager プロセッサーがデプロイされていること
Scans In Progress	http://*IP_address_of_QVM_processor* :8844/rss/scanresults/runningScans.rss	QRadar Vulnerability Manager プロセッサーがデプロイされていること

Docker コンテナーとネットワーク・インターフェース

Docker ネットワークは通信の信頼ゾーン定義します。信頼ゾーンでは、そのネットワーク内にあるコンテナー間の通信が制限されません。

各ネットワークは、ホストのブリッジ・インターフェースに関連付けられています。そしてこれらのインターフェース間のトラフィックをフィルターに掛けるためのファイアウォール・ルールが定義されています。通常、同じ Docker ネットワークとホスト・ブリッジ・インターフェースを共有するゾーン内のコンテナーは、相互に通信できます。同じ `dockerApps` ネットワークで実行しているが、ファイアウォールによって相互に分離されているアプリケーションは、この汎用ルールの例外となります。

Docker インターフェース

Docker インターフェースの例を表示するには、以下のコマンドを入力します。

```
docker network ls
```

出力の例を以下に示します。

```
[root@q1dk00 ~]# docker network ls
NETWORK ID    NAME    DRIVER SCOPE
943dd35a4747 appProxy bridge local
9e2ba36111d1 dockerApps bridge local
```

dockerApps インターフェースは、アプリケーション間の通信に関するルールを適用するために使用します。
appProxy インターフェースは、nginx_framework_apps_proxyコンテナーを表示します。

Docker インターフェースに関する情報

以下のコマンドを入力して Docker インターフェースに関する情報を取得します。

```
docker inspect <docker_container_ID> | grep NetworkMode
```

出力の例を以下に示します。

```
"NetworkMode": "appProxy"
```

この例では、**docker inspect <docker_container_ID>** コマンドをパイプで **less** に渡し、ネットワークの詳細を表示する方法を示します。

```
docker inspect d9b3e58649de | less
```

出力の例を以下に示します。

```
"Networks": {
                            "dockerApps": {
                                "IPAMConfig": null,
                                "Links": null,
                                "Aliases": [
                                    "d9b3e58649de"
                                ], "NetworkID":
 "79bc4716da5139a89cfa5360a3b72824e67701523768822d11b53caeaa5e349e",
                                "EndpointID":
"9dba9d9a174b037f72333945b72cdf60c3719fdb9a3a10a14a8ee3cc0e92a856",
                                "Gateway": "172.18.0.1",
                                "IPAddress": "172.18.0.2",
                                "IPPrefixLen": 16,
                                "IPv6Gateway": "2003:db8:1::1",
                                "GlobalIPv6Address": "2003:db8:1::2",
                                "GlobalIPv6PrefixLen": 64,
                                "MacAddress": "02:42:ac:12:00:02"
                        }
```

この出力例では、指定したコンテナー (d9b3e58649de) で使用されているネットワーク構成が示され、Docker ネットワーク・インターフェース名 (dockerApps) と、Docker コンテナーに関連付けられているネットワーク IP アドレスが示されています。

第 27 章 RESTful API

REST (Representational State Transfer) アプリケーション・プログラミング・インターフェース (API) は、IBM Security QRadar を他のソリューションと統合する際に役に立ちます。QRadar コンソールで特定のエンドポイント (URL) に対して HTTPS 要求を送信することにより、QRadar コンソール上でアクションを実行できます。

各エンドポイントには、アクセスするリソースとそのリソースに対して実行するアクションの URL が含まれます。アクションは、要求の HTTP メソッド (GET、POST、PUT、または DELETE) によって示されます。各エンドポイントのパラメーターと応答について詳しくは、「*IBM Security QRadar API ガイド*」を参照してください。

QRadar API フォーラムとコード・サンプル

API フォーラムでは、よくある質問に対する回答や、テスト環境で使用できるサンプルの注釈付きコードなど、REST API に関する詳細情報を参照することができます。詳しくは、API フォーラム (https://www.ibm.com/developerworks/community/forums/html/forum?id=b02461a3-9a70-4d73-94e8-c096abe263ca) を参照してください。

対話式 API 文書ページへのアクセス

対話式 API 文書ページを使用して、RESTful API の技術的な詳細にアクセスし、サーバーに対する API 要求の実行を試すことができます。

このタスクについて

API 文書ユーザー・インターフェースは、以下の REST API インターフェースの説明と、これらを使用する機能を提供します。

表 108. REST API インターフェース

REST API	説明
/api/analytics	ルールのカスタム・アクションを作成、更新、および削除します。
/api/ariel	イベントおよびフローのプロパティーの表示、イベントおよびフローの検索の作成、検索の管理を行います。
/api/asset_model	モデル内のすべてのアセットのリストを返します。使用可能なすべてのアセット・プロパティー・タイプと保存済み検索をリスト表示したり、アセットを更新したりすることもできます。
/api/auth	現行セッションをログアウトし、無効化する。

表 108. REST API インターフェース (続き)

REST API	説明
/api/config	テナント、ドメイン、および QRadar 拡張を表示および管理します。
/api/gui_app_framework	GUI アプリケーション・フレームワーク Software Development Kit を使用して作成されるアプリケーションをインストールおよび管理します。
/api/help	API 機能のリストに戻る。
/api/qvm	アセット、脆弱性、ネットワーク、オープン・サービス、フィルターを取得します。修復チケットの作成や更新を行うこともできます。
/api/reference_data	リファレンス・データ収集の表示と管理を行います。
/api/scanner	スキャン・プロファイルに関連するリモート・スキャンの表示、作成、開始を行います。
/api/siem	オフェンスを表示、更新、クローズします。メモの追加およびオフェンスのクローズ理由の管理も行えます。
/api/system	サーバー・ホスト、ネットワーク・インターフェース、およびファイアウォール・ルールを管理します。

手順

1. 対話式 API 文書インターフェースにアクセスするには、Web ブラウザーに https://コンソールの *IP* アドレス/api_doc/ という URL を入力します。
2. 使用する API バージョンの横の矢印アイコンをクリックします。

   QRadarV7.3.0 の最新バージョンは 8.0 です。
3. アクセスするエンドポイントに移動します。
4. エンドポイントの文書を読み、要求パラメーターを入力します。
5. 「試用」をクリックし、API 要求をコンソールに送信して、適切にフォーマット設定された HTTPS 応答を受信します。

   注**:** 「試用」をクリックすると、QRadar システム上でアクションが実行されます。一部のアクションは元に戻せません。例えば、クローズしたオフェンスを再オープンすることはできません。
6. QRadar と統合するために必要な情報を検討および収集します。

特記事項

本書は米国 IBM が提供する製品およびサービスについて作成したものです。

本書に記載の製品、サービス、または機能が日本においては提供されていない場合があります。日本で利用可能な製品、サービス、および機能については、日本 IBM の営業担当員にお尋ねください。本書で IBM 製品、プログラム、またはサービスに言及していても、その IBM 製品、プログラム、またはサービスのみが使用可能であることを意味するものではありません。これらに代えて、IBM の知的所有権を侵害することのない、機能的に同等の製品、プログラム、またはサービスを使用することができます。ただし、IBM 以外の製品とプログラムの操作またはサービスの評価および検証は、お客様の責任で行っていただきます。

IBM は、本書に記載されている内容に関して特許権 (特許出願中のものを含む) を保有している場合があります。本書の提供は、お客様にこれらの特許権について実施権を許諾することを意味するものではありません。実施権についてのお問い合わせは、書面にて下記宛先にお送りください。

〒103-8510
東京都中央区日本橋箱崎町19番21号
日本アイ・ビー・エム株式会社
法務・知的財産
知的財産権ライセンス渉外

IBM およびその直接または間接の子会社は、本書を特定物として現存するままの状態で提供し、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任を負わないものとします。国または地域によっては、法律の強行規定により、保証責任の制限が禁じられる場合、強行規定の制限を受けるものとします。

この情報には、技術的に不適切な記述や誤植を含む場合があります。本書は定期的に見直され、必要な変更は本書の次版に組み込まれます。IBM は予告なしに、随時、この文書に記載されている製品またはプログラムに対して、改良または変更を行うことがあります。

本書において IBM 以外の Web サイトに言及している場合がありますが、便宜のため記載しただけであり、決してそれらの Web サイトを推奨するものではありません。それらの Web サイトにある資料は、この IBM 製品の資料の一部ではありません。それらの Web サイトは、お客様の責任でご使用ください。

IBM は、お客様が提供するいかなる情報も、お客様に対してなんら義務も負うことのない、自ら適切と信ずる方法で、使用もしくは配布することができるものとします。

本プログラムのライセンス保持者で、(i) 独自に作成したプログラムとその他のプログラム (本プログラムを含む) との間での情報交換、および (ii) 交換された情報の相互利用を可能にすることを目的として、本プログラムに関する情報を必要とする方は、下記に連絡してください。

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

本プログラムに関する上記の情報は、適切な使用条件の下で使用することができますが、有償の場合もあります。

本書で説明されているライセンス・プログラムまたはその他のライセンス資料は、IBM 所定のプログラム契約の契約条項、IBM プログラムのご使用条件、またはそれと同等の条項に基づいて、IBM より提供されます。

記載されている性能データとお客様事例は、例として示す目的でのみ提供されています。実際の結果は特定の構成や稼働条件によって異なります。

IBM 以外の製品に関する情報は、その製品の供給者、出版物、もしくはその他の公に利用可能なソースから入手したものです。IBM は、それらの製品のテストは行っておりません。したがって、他社製品に関する実行性、互換性、またはその他の要求については確証できません。IBM 以外の製品の性能に関する質問は、それらの製品の供給者にお願いします。

IBM の将来の方向または意向に関する記述については、予告なしに変更または撤回される場合があり、単に目標を示しているものです。

表示されている IBM の価格は IBM が小売り価格として提示しているもので、現行価格であり、通知なしに変更されるものです。卸価格は、異なる場合があります。

本書には、日常の業務処理で用いられるデータや報告書の例が含まれています。より具体性を与えるために、それらの例には、個人、企業、ブランド、あるいは製品などの名前が含まれている場合があります。これらの名称はすべて架空のものであり、名称や住所が類似する企業が実在しているとしても、それは偶然にすぎません。

商標

IBM、IBM ロゴおよび ibm.com® は、世界の多くの国で登録された International Business Machines Corporation の商標です。他の製品名およびサービス名等は、それぞれ IBM または各社の商標である場合があります。現時点での IBM の商標リストについては、http://www.ibm.com/legal/copytrade.shtml をご覧ください。

Linux は、Linus Torvalds の米国およびその他の国における登録商標です。

UNIX は The Open Group の米国およびその他の国における登録商標です。

Java およびすべての Java 関連の商標およびロゴは Oracle やその関連会社の米国およびその他の国における商標または登録商標です。

Microsoft、Windows、Windows NT および Windows ロゴは、Microsoft Corporation の米国およびその他の国における商標です。

製品資料に関するご使用条件

これらの資料は、以下のご使用条件に同意していただける場合に限りご使用いただけます。

適用度

IBM Web サイトの「ご利用条件」に加えて、以下のご使用条件が適用されます。

個人使用

これらの資料は、すべての著作権表示その他の所有権表示をしていただくことを条件に、非商業的な個人による使用目的に限り複製することができます。ただし、IBM の明示的な承諾をえずに、これらの資料またはその一部について、二次的著作物を作成したり、配布 (頒布、送信を含む) または表示 (上映を含む) することはできません。

商業的使用

これらの資料は、すべての著作権表示その他の所有権表示をしていただくことを条件に、お客様の企業内に限り、複製、配布、および表示することができます。ただし、IBM の明示的な承諾をえずにこれらの資料の二次的著作物を作成したり、お客様の企業外で資料またはその一部を複製、配布、または表示することはできません。

権限

ここで明示的に許可されているもの以外に、資料や資料内に含まれる情報、データ、ソフトウェア、またはその他の知的所有権に対するいかなる許可、ライセンス、または権利を明示的にも黙示的にも付与するものではありません。

資料の使用が IBM の利益を損なうと判断された場合や、上記の条件が適切に守られていないと判断された場合、IBM はいつでも自らの判断により、ここで与えた許可を撤回できるものとさせていただきます。

お客様がこの情報をダウンロード、輸出、または再輸出する際には、米国のすべての輸出入 関連法規を含む、すべての関連法規を遵守するものとします。

IBM は、これらの資料の内容についていかなる保証もしません。これらの資料は、特定物として現存するままの状態で提供され、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任なしで提供されます。

IBM オンラインでのプライバシー・ステートメント

サービス・ソリューションとしてのソフトウェアも含めた IBM ソフトウェア製品 (「ソフトウェア・オファリング」) では、製品の使用に関する情報の収集、エンド・ユーザーの使用感の向上、エンド・ユーザーとの対話またはその他の目的のために、Cookie はじめさまざまなテクノロジーを使用することがあります。多くの場合、ソフトウェア・オファリングにより個人情報が収集されることはありません。IBM の「ソフトウェア・オファリング」の一部には、個人情報を収集できる機能を持つものがあります。ご使用の「ソフトウェア・オファリング」が、これらの Cookie およびそれに類するテクノロジーを通じてお客様による個人情報の収集を可能にする場合、以下の具体的事項を確認ください。

このソフトウェア・オファリングは、展開される構成に応じて、セッション管理および認証の目的のために、それぞれのお客様のセッション ID を、セッションごとの Cookie を使用して収集する場合があります。これらの Cookie は無効にできますが、その場合、これらを有効にした場合の機能を活用することはできません。

この「ソフトウェア・オファリング」が Cookie およびさまざまなテクノロジーを使用してエンド・ユーザーから個人を特定できる情報を収集する機能を提供する場合、 お客様は、このような情報を収集するにあたって適用される法律、ガイドライン等を遵守する必要があります。これには、エンドユーザーへの通知や同意の要求も含まれますがそれらには限られません。

このような目的での Cookie を含む様々なテクノロジーの使用の詳細については、IBM の『IBM オンラインでのプライバシー・ステートメント』(http://www.ibm.com/privacy/details/jp/ja/) の『クッキー、ウェブ・ビーコン、その他のテクノロジー』および『IBM Software Products and Software-as-a-Service Privacy Statement』(http://www.ibm.com/software/info/product-privacy) を参照してください。

用語集

この用語集には、IBM Security QRadar SIEM のソフトウェアおよび製品で使用する用語と定義を記載します。

この用語集では、以下の相互リファレンスを使用しています。

- 「～を参照」という表現は、非優先用語の場合は優先用語を参照し、略語の場合は正式な用語を参照するように促すための表現です。
- 「～も参照」という表現は、関連する用語や対比的な用語を参照するように促すための表現です。

この用語集に記載されていない用語と定義については、IBM Terminology Web サイト (新しいウィンドウで開きます) を参照してください。

A

アキュムレーター **(accumulator)**
特定の操作の 1 つのオペランドを格納するためのレジスター。このオペランドは、この操作の実行結果によって置き換えられる。

アクティブ・システム **(active system)**
高可用性 (HA) クラスターにおいて、すべてのサービスが稼働しているシステム。

アドレス解決プロトコル **(ARP) (Address Resolution Protocol (ARP))**
ローカル・エリア・ネットワーク内で IP アドレスをネットワーク・アダプター・アドレスに動的にマップするプロトコル。

管理共有 **(administrative share)**
管理特権のないユーザーに非表示になっているネットワーク・リソース。管理共有により、管理者はネットワーク・システム上のすべてのリソースにアクセスできる。

アノマリ **(anomaly)**
正常なネットワーク振る舞いから逸脱した振る舞い。

アプリケーション・シグニチャー **(application signature)**
パケット・ペイロードの検証によって取得された一連の固有の特性。特定のアプリケーションを識別するために使用される。

ARP 「アドレス解決プロトコル (Address Resolution Protocol)」を参照。

ARP リダイレクト **(ARP Redirect)**
ネットワーク上に問題が存在する場合に、その問題をホストに通知するための ARP 方式。

ASN 「自律システム番号 (autonomous system number)」を参照。

アセット **(asset)**
稼働環境にデプロイされているか、デプロイされる予定の管理可能オブジェクト。

自律システム番号 **(ASN) (autonomous system number (ASN))**
TCP/IP において、IP アドレスの割り当てを行う同じ中央認証局によって自律システムに割り当てられた番号。自律システム番号を自動ルーティング・アルゴリズムで使用すると、自律システムを識別することができる。

B

振る舞い **(behavior)**
特定の操作やイベントについて、その結果を含めた監視可能な影響。

結合インターフェース **(bonded interface)**
「リンク集約 (link aggregation)」を参照。

バースト **(burst)**
ライセンス交付を受けたフローやイベントの速度制限を超えるような、着信イベントまたはフローの突然で急激な増加。

C

CIDR 「クラスレス・ドメイン間ルーティング (Classless Inter-Domain Routing)」を参照。

クラスレス・ドメイン間ルーティング **(CIDR) (Classless Inter-Domain Routing (CIDR))**
クラス C のインターネット・プロトコル (IP) アドレスを追加するための方式。アドレスはインターネット・サービス・プロバイダー (ISP) に渡され、そのプロバイダーのユーザーによって使用される。CIDR アドレスによってルーティング・テーブルのサイズが削減されるため、組織内でより多くの IP アドレスを使用できるようになる。

クライアント **(client)**
サーバーからのサービスを要求するソフトウェア・プログラムまたはコンピューター。

クラスター仮想 **IP** アドレス **(cluster virtual IP address)**
プライマリー・ホストまたはセカンダリー・ホストと HA クラスターとの間で共有される IP アドレス。

統合間隔 **(coalescing interval)**
イベントをバンドルする間隔。イベントのバンドルは 10 秒間隔で実行され、現在のいずれの統合イベントにも一致しない最初のイベントから開始される。統合間隔の間に、一致する最初の 3 つのイベントがバンドルされ、イベント・プロセッサー・プログラムに送信される。

共通脆弱性評価システム **(CVSS) (Common Vulnerability Scoring System (CVSS))**
脆弱性の重大度を測定するための評価システム。

コンソール **(console)**
オペレーターがシステム操作の制御と監視を行うためのディスプレイ装置。

コンテンツ・キャプチャー **(content capture)**
構成可能なペイロード量を取得し、そのデータをフロー・ログに格納するプロセス。

資格情報 **(credential)**
ユーザーまたはプロセスに対して特定のアクセス権を付与する情報のセット。

信頼性 **(credibility)**
イベントやオフェンスの保全性を判別するために使用される 0 から 10 までの数値による評価。複数のソースから同じイベントやオフェンスが報告されると、信頼性が高くなる。

CVSS 「共通脆弱性評価システム (Common Vulnerability Scoring System)」を参照。

D

データベース・リーフ・オブジェクト **(database leaf object)**
データベース階層内の終端のオブジェクトまたはノード。

データ・ポイント **(datapoint)**
特定の時点におけるメトリックの計算値。

デバイス・サポート・モジュール **(DSM) (Device Support Module (DSM))**
複数のログ・ソースから受信したイベントを解析し、出力として表示可能な標準分類形式に変換する構成ファイル。

DHCP
「動的ホスト構成プロトコル (Dynamic Host Configuration Protocol)」を参照。

DNS 「ドメイン・ネーム・システム (Domain Name System)」を参照。

ドメイン・ネーム・システム **(DNS) (Domain Name System (DNS))**
ドメイン名を IP アドレスにマップする分散データベース・システム。

DSM 「デバイス・サポート・モジュール (Device Support Module)」を参照。

重複フロー **(duplicate flow)**
異なる複数のフロー・ソースから受信した、同じデータ伝送の複数のインスタンス。

動的ホスト構成プロトコル **(DHCP) (Dynamic Host Configuration Protocol (DHCP))**
構成情報を一元的に管理するために使用される通信プロトコル。例えば DHCP は、

ネットワーク内のコンピューターに対して自動的に IP アドレスを割り当てる。

E

暗号化 **(encryption)**
コンピューター・セキュリティーにおいて、元のデータを取得できないように判読不能な形式にデータを変換するプロセス。暗号化解除プロセスを使用しない限り、元のデータを取得することはできない。

エンドポイント **(endpoint)**
環境内の API またはサービスのアドレス。API は、エンドポイントを公開し、同時に他のサービスのエンドポイントを呼び出す。

外部スキャン・アプライアンス **(external scanning appliance)**
ネットワーク内のアセットに関する脆弱性情報を収集するためにネットワークに接続されているマシン。

F

フォールス・ポジティブ **(false positive)**
オフェンスを作成しないとユーザーが判断できるイベントまたはフロー。あるいは、セキュリティー・インシデントではないとユーザーが判断するオフェンス。

フロー **(flow)**
対話時にリンク経由で通過するデータの 1 回の伝送。

フロー・ログ **(flow log)**
フロー・レコードの集合。

フロー・ソース **(flow sources)**
フローの取得元。管理対象ホストにインストールされているハードウェアからフローが発生している場合、フロー・ソースは内部フローとして分類され、フローがフロー・コレクターに送信される場合は、外部フローとして分類される。

宛先転送 **(forwarding destination)**
正規化された生データをログ・ソースとフロー・ソースから受信する 1 つ以上のベンダー・システム。

FQDN
「完全修飾ドメイン名 (fully qualified domain name)」を参照。

FQNN
「完全修飾ネットワーク名 (fully qualified network name)」を参照。

完全修飾ドメイン名 **(FQDN) (fully qualified domain name (FQDN))**
インターネット通信において、ドメイン名のサブネームをすべて含むホスト・システム名。完全修飾ドメイン名の例としては、rchland.vnet.ibm.com などがある。

完全修飾ネットワーク名 **(FQNN) (fully qualified network name (FQNN))**
ネットワーク階層において、すべての部門を含むオブジェクトの名前。完全修飾ネットワーク名の例としては、CompanyA.Department.Marketing などがある。

G

ゲートウェイ **(gateway)**
ネットワーク体系が異なるネットワークやシステムの接続に使用されるデバイスまたはプログラム。

H

HA 「高可用性 (high availability)」を参照。

HA クラスター **(HA cluster)**
1 台のプライマリー・サーバーと 1 台のセカンダリー・サーバーで構成される高可用性構成。

ハッシュ・ベース・メッセージ認証コード **(HMAC) (Hash-Based Message Authentication Code (HMAC))**
暗号ハッシュ機能と秘密鍵を使用する暗号コード。

高可用性 **(HA) (high availability (HA))**
特定のノードまたはデーモンで障害が発生した場合に、ワークロードをクラスター内の他のノードに再配分できるように再構成されるクラスター化システムに関連する構成。

HMAC
「ハッシュ・ベース・メッセージ認証コード (Hash-Based Message Authentication Code)」を参照。

ホスト・コンテキスト **(host context)**
コンポーネントをモニターし、各コンポーネントが正常に機能していることを確認するサービス。

I

ICMP 「Internet Control Message Protocol」を参照。

アイデンティティー **(identity)**
人、組織、場所、項目を表す、データ・ソースの属性の集合。

IDS 「侵入検知システム (intrusion detection system)」を参照。

Internet Control Message Protocol (ICMP)
データグラムのエラーを報告するなどの目的でソース・ホストと通信する際に、ゲートウェイが使用するインターネット・プロトコル。

インターネット・プロトコル **(IP) (Internet Protocol (IP))**
ネットワークまたは相互接続ネットワーク経由でデータを送信するプロトコル。このプロトコルは、上位のプロトコル層と物理ネットワークとの間の中継役として機能する。「伝送制御プロトコル (Transmission Control Protocol)」も参照。

インターネット・サービス・プロバイダー **(ISP) (Internet service provider (ISP))**
インターネットへのアクセスを提供する組織。

侵入検知システム **(IDS) (intrusion detection system (IDS))**
ネットワークやホスト・システムの一部であるモニター対象リソース上での侵入の試みや実際の侵入を検出するソフトウェア。

侵入防止システム **(IPS) (intrusion prevention system (IPS))**
潜在的な悪意を持つアクティビティーを拒否するシステム。拒否の手段としては、フィルター処理、トラッキング、速度制限の設定などがある。

IP 「インターネット・プロトコル (Internet Protocol)」を参照。

IP マルチキャスト **(IP multicast)**
単一のマルチキャスト・グループを構成する一連のシステムに対するインターネット・プロトコル (IP) データグラムの伝送。

IPS 「侵入防止システム (intrusion prevention system)」を参照。

ISP 「インターネット・サービス・プロバイダー (Internet service provider)」を参照。

K

鍵ファイル **(key file)**
コンピューター・セキュリティーにおいて、公開鍵、秘密鍵、トラステッド・ルート、および証明書を含むファイル。

L

L2L 「ローカルからローカル (Local To Local)」を参照。

L2R 「ローカルからリモート (Local To Remote)」を参照。

LAN ローカル・エリア・ネットワーク (Local Area Network) を参照してください。

LDAP
「Lightweight Directory Access Protocol」を参照。

リーフ **(leaf)**
ツリーにおいて、子を持たないエントリーまたはノード。

Lightweight Directory Access Protocol (LDAP)
TCP/IP を使用して、ディレクトリーへのアクセスを提供するオープン・プロトコル。X.500 モデルをサポートし、より複雑な X.500 Directory Access Protocol (DAP) のリソース要件には制約されない。例えば、LDAP を使用して、インターネット・ディレクトリーまたはイントラ

ネット・ディレクトリーで個人や組織などのリソースを検索することができる。

リンク集約 **(link aggregation)**
ケーブルやポートなどの物理ネットワーク・インターフェース・カードの、単一の論理ネットワーク・インターフェースへのグループ化。リンク集約は、帯域幅およびネットワーク可用性を増大させるために使用される。

ライブ・スキャン **(live scan)**
セッション名に基づいてスキャン結果からレポート・データを生成する脆弱性スキャン。

ローカル・エリア・ネットワーク **(LAN) (local area network (LAN))**
限定された領域内 (単一のビルやキャンパスなど) の複数のデバイスを接続するネットワーク。このネットワークを、さらに大きなネットワークに接続することができる。

ローカルからローカル **(L2L) (Local To Local (L2L))**
あるローカル・ネットワークから別のローカル・ネットワークへの内部トラフィックに関連する構成。

ローカルからリモート **(L2R) (Local To Remote (L2R))**
あるローカル・ネットワークから別のリモート・ネットワークへの内部トラフィックに関連する構成。

ログ・ソース **(log source)**
イベント・ログの発生元となるセキュリティー装置またはネットワーク装置。

ログ・ソース拡張 **(log source extension)**
イベント・ペイロードからのイベントを識別し分類するために必要な正規表現パターンをすべて格納している XML ファイル。

M

判定機能 **(Magistrate)**
定義されているカスタム・ルールに対してネットワーク・トラフィックとセキュリティー・イベントを分析する内部コンポーネント。

マグニチュード **(magnitude)**
特定のオフェンスの相対的な重要度の尺度。マグニチュードは、関連性、重大度、信頼性から算出された重みを持つ値である。

N

NAT 「ネットワーク・アドレス変換 (network address translation)」を参照。

NetFlow
ネットワーク・トラフィックのフロー・データをモニターする Cisco ネットワーク・プロトコル。 NetFlow データには、クライアントとサーバーの情報、使用されるポート、ネットワークに接続されているスイッチとルーターを通過するバイト数とパケット数が含まれている。このデータは NetFlow コレクターに送信され、NetFlow コレクターがデータの分析を行う。

ネットワーク・アドレス変換 **(NAT) (network address translation (NAT))**
ファイアウォールにおいて、セキュアなインターネット・プロトコル (IP) アドレスを外部の登録済みアドレスに変換すること。これにより、外部ネットワークとの通信が可能になり、ファイアウォール内部で使用される IP アドレスはマスクされる。

ネットワーク階層 **(network hierarchy)**
ネットワーク・オブジェクトの階層コレクションであるコンテナーのタイプ。

ネットワーク層 **(network layer)**
OSI アーキテクチャーにおいて、予測可能なサービス品質を持つ複数のオープン・システム間でパスを確立するためのサービスを提供する層。

ネットワーク・オブジェクト **(network object)**
ネットワーク階層のコンポーネント。

O

オフェンス **(offense)**
モニター対象の条件に対する応答として送信されたメッセージまたは生成されたイベント。オフェンスは、ポリシー違反があっ

たかどうか、ネットワークが攻撃されているかどうかなどの情報を提供します。

オフサイト・ソース **(offsite source)**
正規化されたデータをイベント・コレクターに転送する、プライマリー・サイトから離れた場所に存在するデバイス。

オフサイト・ターゲット **(offsite target)**
イベント・コレクターからイベント・フローまたはデータ・フローを受信する、プライマリー・サイトから離れた場所に存在するデバイス。

オープン・ソース脆弱性データベース **(OSVDB) (Open Source Vulnerability Database (OSVDB))**
ネットワーク・セキュリティー・コミュニティーがネットワーク・セキュリティー・コミュニティーのために作成した、ネットワーク・セキュリティーの脆弱性に関する技術情報を提供するオープン・ソース・データベース。

オープン・システム間相互接続 **(OSI) (open systems interconnection (OSI))**
国際標準化機構 (ISO) の標準に準拠した、情報交換のためのオープン・システムの相互接続。

OSI 「オープン・システム間相互接続 (open systems interconnection」を参照。

OSVDB
「オープン・ソース脆弱性データベース (Open Source Vulnerability Database)」を参照。

P

解析順序 **(parsing order)**
共通の IP アドレスまたはホスト名を共有するログ・ソースに対して、ユーザーが重要度の順序を定義できるログ・ソース定義。

ペイロード・データ **(payload data)**
IP フローに含まれるアプリケーション・データ。ただし、ヘッダーと管理情報は除く。

プライマリー **HA** ホスト **(primary HA host)**
HA クラスターに接続されるメイン・コンピューター。

プロトコル **(protocol)**
通信ネットワーク内の複数のデバイス間またはシステム間におけるデータの通信と転送を制御する一連のルール。

Q

QID マップ **(QID Map)**
それぞれの固有イベントを特定し、そのイベントを下位カテゴリーと上位カテゴリーにマップして、イベントの相関方法と編成方法を決定する分類法。

R

R2L 「リモートからローカル (Remote To Local)」を参照。

R2R 「リモートからリモート (Remote To Remote)」を参照。

recon 「スキャン行為 (reconnaissance)」を参照。

スキャン行為 **(recon) (reconnaissance (recon))**
ネットワーク・リソースの ID に関連する情報を収集する方式。ネットワーク・スキャンやその他の技法を使用してネットワーク・リソース・イベントのリストがコンパイルされ、それらに重大度レベルが割り当てられる。

リファレンス・マップ **(reference map)**
1 つのキーを 1 つの値に直接マップするデータ・レコード。例えば、ユーザー名とグローバル ID とのマッピング。

マップのリファレンス・マップ **(reference map of maps)**
2 つのキーを多数の値にマップするデータ・レコード。例えば、1 つのアプリケーションの合計バイト数と 1 つの送信元 IP とのマッピング。

セットのリファレンス・マップ **(reference map of sets)**
1 つのキーを多数の値にマップするデー

タ・レコード。例えば、特権ユーザーのリストと 1 つのホストとのマッピング。

リファレンス・セット **(reference set)**
ネットワーク上のイベントまたはフローから派生した単一エレメントのリスト。例えば、IP アドレスのリストやユーザー名のリスト。

リファレンス・テーブル **(reference table)**
割り当てられたタイプを持つキーを別のキーにマップするようにデータが記録されるテーブル。この別のキーは、次に、単一値にマップされる。

最新表示タイマー **(refresh timer)**
一定の間隔で、手動または自動でトリガーされる内部デバイス。このデバイスにより、現在のネットワーク・アクティビティー・データが更新される。

関連性 **(relevance)**
ネットワーク上のイベント、カテゴリー、オフェンスの相対的な影響の尺度。

リモートからローカル **(R2L) (Remote To Local (R2L))**
リモート・ネットワークからローカル・ネットワークへの外部トラフィック。

リモートからリモート **(R2R) (Remote To Remote (R2R))**
あるリモート・ネットワークから別のリモート・ネットワークへの外部トラフィック。

レポート **(report)**
クエリー管理において、照会の実行結果にフォームを適用したフォーマット済みデータ。

レポート間隔 **(report interval)**
構成可能な時間間隔。この間隔の最後に、イベント・プロセッサー・プログラムは、取得したすべてのイベント・データとフロー・データをコンソールに送信する。

ルーティング・ルール **(routing rule)**
イベント・データによって基準が満たされた場合に、条件の集合とその結果として発生するルーティングが実行される条件。

ルール **(rule)**
コンピューター・システムが関係を識別し、それに応じて、自動化された応答を実行できるようにする一連の条件ステートメント。

S

スキャナー **(scanner)**
Web アプリケーション内でソフトウェアの脆弱性を検索する、自動化されたセキュリティー・プログラム。

セカンダリー **HA** ホスト **(secondary HA host)**
HA クラスターに接続されるスタンバイ・コンピューター。プライマリー HA ホストで障害が発生した場合は、セカンダリー HA ホストがプライマリー HA ホストの処理を引き継ぐ。

重大度 **(severity)**
送信元が宛先に及ぼす相対的な脅威の尺度。

Simple Network Management Protocol (SNMP)
複雑なネットワーク内のシステムとデバイスをモニターするための一連のプロトコル。管理対象デバイスに関する情報は、管理情報ベース (MIB) で定義されて保管される。

SNMP
「Simple Network Management Protocol」を参照。

SOAP
非集中型の分散環境で情報を交換するための XML ベースの軽量プロトコル。SOAP を使用して、インターネット経由で情報を照会して情報を返し、サービスを呼び出すことができる。

スタンバイ・システム **(standby system)**
アクティブなシステムで障害が発生した場合に、自動的にアクティブになるシステム。ディスクの複製が有効になっている場合、スタンバイ・システムはアクティブなシステムからデータを複製する。

サブネット **(subnet)**
「サブネットワーク (subnetwork)」を参照。

サブネット・マスク **(subnet mask)**
インターネット・サブネットワークで、IP アドレスのホスト部分のサブネットワーク・アドレス・ビットの識別に使用される 32 ビットのマスク。

サブネットワーク **(subnet) (subnetwork (subnet))**
相互に接続された、より小さな独立したサブグループに分割されているネットワーク。

サブ検索 **(sub-search)**
完了した検索結果セット内での検索照会の実行を可能にする機能。

スーパーフロー **(superflow)**
ストレージの制約を減らすことによって処理能力を上げるための、類似するプロパティーを持つ複数のフローから構成される単一のフロー。

システム・ビュー **(system view)**
システムを構成するプライマリー・ホストと管理対象ホストの視覚的な表現。

T

TCP 「伝送制御プロトコル (Transmission Control Protocol)」を参照。

伝送制御プロトコル **(TCP) (Transmission Control Protocol (TCP))**
インターネットで使用される通信プロトコル。また、インターネットワーク・プロトコル用の Internet Engineering Task Force (IETF) 標準に準拠するネットワークでも使用される。TCP は、パケット交換通信ネットワークと、パケット交換通信ネットワークの相互接続システムにおいて、信頼できるホスト間プロトコルを提供する。 「インターネット・プロトコル (Internet Protocol)」も参照。

トラストストア・ファイル **(truststore file)**
トラステッド・エンティティーの公開鍵が入っている鍵データベース・ファイル。

V

違反 **(violation)**
企業のポリシーをバイパスする行為、または企業のポリシーに違反する行為。

脆弱性 **(vulnerability)**
オペレーティング・システム、システム・ソフトウェア、またはアプリケーション・ソフトウェア・コンポーネントでの機密漏れ。

W

whois サーバー **(whois server)**
ドメイン名や IP アドレスの割り振りなど、登録されているインターネット・リソースに関する情報の取得に使用されるサーバー。

索引

日本語, 数字, 英字, 特殊文字の順に配列されています。なお, 濁音と半濁音は清音と同等に扱われています。

[ア行]

[カ行]

[サ行]

[タ行]

[ナ行]

[ハ行]

[マ行]

[ヤ行]

[ラ行]

A

C

D

E

F

I

J

L

M

N

P

Q

S

T

V

Printed in Japan

日本アイ・ビー・エム株式会社
〒103-8510 東京都中央区日本橋箱崎町19-21