IBM Security QRadar SIEM

バージョン 7.2.6

管理ガイド

注記

本書および本書で紹介する製品を使用する前に、 399 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 V7.2.6 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 SIEM
Version 7.2.6
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。

技術文書

Web 上で IBM Security QRadar の製品資料 (翻訳されたすべての資料を含む) を検索するには、 IBM Knowledge Center (http://www.ibm.com/support/knowledgecenter/SS42VS/welcome) にアクセスしてください。

QRadar 製品ライブラリー内の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、企業内および企業外からの不適切なアクセスの防止、検出、およびそれらのアクセスへの対応により、システムおよび情報を保護する必要があります。不適切なアクセスにより、情報が改ざん、破壊、盗用、または悪用されたり、あるいはご使用のシステムの損傷または他のシステムへの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。

注意事項:

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 V7.2.6 の管理に関する新機能

IBM Security QRadar V7.2.6 には、以下の機能と改善点が追加されています。

QRadar のマルチテナント・インスタンスのデプロイおよび管理

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のサービス・プロバイダーが、IBM Security QRadar のマルチテナント・インスタンスをデプロイできるようになっています。カスタマーごとにドメインおよびテナントを作成することによって、各カスタマーを独立して管理することができ、各テナントのユーザーにしかデータが表示されないようにすることができます。 詳細...

IBM Security App Exchange ポータルでの QRadar セキュリティー・コンテンツの共有および共同作業

IBM Security App Exchange は新しい Web ポータルであり、ユーザーやビジネス・パートナーが QRadar グローバル・コミュニティーの能力や知識を活用することができます。IBM Security App Exchange は、他のユーザーと協力したり、必要に応じて利用できる小規模な拡張の形でセキュリティー・コンテンツを共有して QRadar フレームワークの既存の機能を拡張したりするために使用します。 詳細...

QRadar からの機密データの直接的隠蔽

コマンド・ラインを使用せずに QRadar から機密データを直接非表示にするには、新しい「データ難読化管理」ツールを使用します。

新しい事前定義のフィールド・ベースの式により、ユーザー名、グループ名、netBIOS 名、ホスト名などの共通データ・エレメントを容易にマスクできます。また、会社や自治体のプライバシー・ポリシーに従って、イベント・ログおよびフロー・ログ内の他のデータを難読化する正規表現を作成することもできます。 詳細...

コンテンツ管理スクリプトを使用しない拡張とコンテンツのインポート

QRadar の機能を拡張するには、新しい「拡張の管理」ツールを使用して、セキュリティー拡張を QRadar デプロイメントにインポートします。この新しいインターフェースにより、簡単に新しい IBM Security App Exchange から QRadar に直接アプリケーションやセキュリティー・コンテンツを追加したりインストールすることができます。拡張をインストールする前に、コンテンツを確認して、既存のコンテンツを上書きするか保持するかを指定できます。 詳細...

デプロイメントの視覚図

「デプロイメント・アクション」リストから、ホスト・レベルのデプロイメントの視覚図を開くことができます。視覚図では、実際のデプロイメント構成を変更することなく、ホスト間の関係を確認し、ホストの相対的な場所を変更できます。グラフィックは、PNG 形式または VDX 形式のいずれかでエクスポートすることもできます。 詳細...

複数の E メール通知テンプレート

ルールを構成するときに、使用可能な応答 E メール・テンプレートのリストから選択できるようになっています。ユーザーごとに別のテンプレートを作成したり、オフェンス・タイプごとに別のテンプレートを作成したりすることができます。ルールの構成について詳しくは、「*IBM Security QRadar* ユーザーズ・ガイド」を参照してください。 詳細...

リファレンス・データの期限切れイベント

リファレンス・データ・マップ、セットのマップ、マップのマップ、リファレンス・テーブル、およびリファレンス・セットのエレメントで、エレメントの期限が切れたときに「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るようになりました。この「リファレンス・データの期限切れ **(Reference Data Expiry)**」イベントには、収集の名前と期限の切れたエレメントが含まれています。

この機能を使用して、例えば、ネットワーク内の期限切れユーザー・アカウントを追跡したりすることができます。 詳細...

カスタム・アクション・スクリプト

ネットワーク・イベントに対する応答としてカスタム・アクションを実行するスクリプトをカスタム・ルールに追加できます。例えば、ログイン試行の失敗回数を定義し、それによってトリガーされるルールへの応答として、ご使用のネットワークからあるソース IP アドレスをブロックするファイアウォール・ルールを作成するスクリプトを作成できます。「管理」タブの「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・スクリプトを管理できます。 詳細...

システム設定のセキュリティー向上

システム設定は、セキュリティーが強化された新しいインターフェースで構成します。新しい「システムの表示と管理」ウィンドウに HTTPS でアクセスし、ファイアウォール、ネットワーク・インターフェース、および E メール・サーバーを構成します。

注: セキュリティーを強化するために、QRadar コンソールでシステム時刻およびパスワード変更を構成してください。 詳細...

非アクティブ・タイムアウト

「非アクティブ・タイムアウト」プロパティーで、アクティブでないセッションが存続する最大時間を制御します。アクティビティーがないまま指定された時間が経過すると、セッションが終了し、ユーザーはログアウトされます。デフォルトの最大時間は 30 分です。 詳細...

第 2 章 QRadar 管理の概要

管理者は、IBM Security QRadar の「管理」タブを使用して、ダッシュボード、ログ・アクティビティー、オフェンス、ネットワーク・アクティビティー、アセット (存在する場合)、およびレポートを管理します。

この概要には、ユーザー・インターフェースおよび「管理」タブへのアクセスの仕方と使用法についての一般的な情報が含まれています。

ご使用のセキュリティー・インテリジェンス製品の機能

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 Security QRadar SIEM には、オンプレミス・デプロイメントのための全範囲のセキュリティー・インテリジェンス機能が含まれます。QRadar SIEM は、ネットワーク上に分散しているデバイス・エンドポイントとアプリケーションからのログ・ソース・イベント・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誤検知を区別します。

IBM Security Intelligence on Cloud を使用すると、ホスト環境で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、アーカイブ、および保管できます。データを分析して発展しつつある脅威を可視化すること、およびコンプライアンスのモニタリングおよびレポートの要件に対応することができ、一方で総所有コスト (TCO) を削減できます。

IBM Security QRadar Log Manager を使用すると、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、アーカイブ、および保管できます。QRadar Log Manager を使用すると、データを分析して発展しつつある脅威を可視化すること、およびコンプライアンスのモニタリングおよびレポートの要件に対応することができます。

支援が必要な場合、製品の機能がリストされている次の表を使用してください。

表 *1. QRadar* の機能の比較

機能	**QRadar SIEM**	**IBM Security Intelligence on Cloud**	**IBM Security QRadar Log Manager**
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

表 1. *QRadar* の機能の比較 (続き)

機能	**QRadar SIEM**	**IBM Security Intelligence on Cloud**	**IBM Security QRadar Log Manager**
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	いいえ	はい
ネットワーク・アクティビティー・モニタリング	はい	いいえ	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。

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。

QRadar システムにアクセスすると、ユーザー名とパスワードの入力を求められます。このユーザー名とパスワードは、管理者が事前に構成しておく必要があります。

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	38.0 延長サポート版

表 2. *QRadar* 製品でサポートされる *Web* ブラウザー (続き)

Web ブラウザー	サポート対象のバージョン
32 ビット版または 64 ビット版の Microsoft Internet Explorer (ドキュメント・モードまたはブラウザー・モードを有効にすること)。	10.0
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	バージョン 46

「管理」タブの概要

「管理」タブには、いくつかのタブとメニューのオプションがあり、これらを使用して、QRadar を構成することができます。

管理機能にアクセスするには管理特権が必要です。管理機能にアクセスするには、ユーザー・インターフェースの「管理」タブをクリックします。

「管理」タブには、以下のメニュー・メニューもあります。

表 3. 「管理」タブ・メニューのオプション

メニュー・オプション	説明
デプロイメント・エディター	「デプロイメント・エディター」ウィンドウを開きます。詳しくは、 149 ページの『第 11 章 デプロイメント・エディター』を参照してください。
変更のデプロイ	現行セッションからの構成変更をデプロイメントにデプロイします。詳しくは、 8 ページの『変更のデプロイ』を参照してください。
拡張	「拡張」メニューには、以下のオプションがあります。 「**SIM** モデルのクリーンアップ」 - SIM モジュールをリセットします。 9 ページの『SIM のリセット』を参照してください。 「すべての構成のデプロイ」 - すべての構成変更をデプロイします。 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。詳しくは、 8 ページの『変更のデプロイ』を参照してください。

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たび、また、「管理」タブでウィンドウを閉じるたびに、「管理」タブの上部のバナーに**「デプロイされていない変更を検査しています」**というメッセージが表示されます。デプロイされていない変更が見つかると、バナーが更新されて、デプロイされていない変更についての情報が表示されます。

デプロイされていない変更のリストが非常に長い場合、スクロール・バーが表示されます。リストをスクロールしてください。

バナーのメッセージには、推奨されるデプロイメント変更のタイプも示されます。2 つのオプションのうち、いずれか 1 つを選択してください。

- 「変更のデプロイ」 - 「管理」タブのツールバーにある「変更のデプロイ」アイコンをクリックすると、現行セッションからのすべての構成変更がデプロイメントにデプロイされます。
- 「すべての構成のデプロイ」 - 「管理」タブのメニューから「拡張」 > 「すべての構成のデプロイ」を選択すると、すべての構成設定がデプロイメントにデプロイされます。その後、デプロイされたすべての変更が、デプロイメント全体に適用されます。

  重要**:** 「すべての構成のデプロイ」をクリックすると、QRadar はすべてのサービスを再開します。このため、デプロイが完了するまで、データ収集にギャップが生じます。

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、ステージング・エリアで再度チェックされます。デプロイされていない変更がない場合、**「デプロイする変更がありません。」**というメッセージが表示されます。

手順

1. 「詳細の表示」をクリックします。
2. 次のオプションのいずれかを選択してください。
   a. 1 つのグループを展開してすべての項目を表示するには、テキストの横にある正符号 (+) をクリックします。展開されているときは、負符号 (-) をクリックすることができます。
   b. すべてのグループを展開するには、「すべて展開」をクリックします。展開されているときは、「すべて省略」をクリックすることができます。
   c. 「詳細を表示しない」をクリックすると、同様にビューに詳細が表示されなくなります。
3. 以下の推奨されるタスクを実行します。
   a. 「管理」タブ・メニューで、「変更のデプロイ」をクリックします。
   b. 「管理」タブ・メニューから、「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。

ユーザー詳細の更新

メイン・ユーザー・インターフェースを使用して、管理ユーザーの詳細にアクセスすることができます。

手順

1. 「設定」をクリックします。
2. 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 **(**確認**)**	新規パスワードを再度入力します。
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。 ポップアップ通知について詳しくは、製品の「ユーザー・ガイド」を参照してください。

3. 「保存」をクリックします。

SIM のリセット

「管理」を使用して、SIM モジュールをリセットします。これで、すべてのオフェンス、送信元 IP アドレス、および宛先 IP アドレスの情報をデータベースとディスクから削除することができます。

このタスクについて

このオプションは、フォールス・ポジティブ情報をさらに受信しないようにするために、デプロイメントをチューニングした後に役立ちます。

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、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」ウィンドウの情報を確認します。

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. SIM のリセット・プロセスが完了したら、ブラウザーをリセットします。

SNMP でのシステムのモニター

SNMP ポーリングを使用したアプライアンスのモニター。

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。

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。システム・パフォーマンスを向上させるために、集約データ・ビューの無効化、有効化、削除を実行できます。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」ドロップダウン・リストの項目によって、表示されるデータがソートし直されます。

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. 「集約データ管理」アイコンをクリックします。
4. 集約データ・ビューのリストをフィルターに掛けるには、次のいずれかのオプションを選択します。
   - 次のリストからいずれかのオプションを選択します。「ビュー」、「データベース」、「表示」、または「表示」。
   - 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。
5. 集約データ・ビューを管理するには、そのビューを選択し、ツールバーから該当するアクションを選択します。
   - 「ビューの無効化」または「ビューの削除」を選択した場合、ウィンドウに、集合データ・ビューのコンテンツの依存関係が表示されます。集約データ・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。
   - 無効にした集約データ・ビューを有効にすると、削除されたビューの集約データが復元されます。

表 4. 「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
有効な固有の数	True または False。一定時間における平均カウントではなく、固有のイベントとフローのカウントが検索結果に表示されます。

RESTful API

Representational State Transfer (REST) 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、HTTPS 照会を作成し、IBM Security QRadar を他のソリューションに統合します。

アクセス権限とユーザー・ロール権限

RESTful API にアクセスして使用するには、QRadar で管理ユーザー・ロール権限が付与されている必要があります。

REST API 技術資料ユーザー・インターフェースへのアクセス

API 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機能を提供します。

表 5. *REST API* インターフェース

REST API	説明
/api/ariel	データベース、検索、検索 ID、および検索結果を照会する。
/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。
/api/help	API 機能のリストに戻る。
/api/siem	すべてのオフェンスのリストを返します。
/api/qvm	QRadar Vulnerability Manager データの確認と管理を行います。
/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/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/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。

REST API の技術資料インターフェースに備わっているフレームワークを使用して、QRadar の機能を他の製品に実装するために必要なコードを収集できます。

1. 技術資料インターフェースにアクセスするには、Web ブラウザーで https://コンソールの *IP* アドレス/api_doc という URL を入力してください。
2. アクセスしたい API のヘッダーをクリックします (例えば **/ariel**)。
3. アクセスしたいエンドポイントのサブヘッダーをクリックします (例えば **/databases**)。
4. サブヘッダー「Experimental」または「Provisional」をクリックします。

   注**:**

   API エンドポイントには、*experimental* または *stable* といういずれかの注釈が付けられます。

   Experimental
   API エンドポイントが完全にはテストされておらず、将来予告なしに変更または削除される可能性があることを示します。

Stable

API エンドポイントが完全にテストされ、サポートされていることを示します。

5. 「**Try it out**」をクリックして、適切な形式の HTTPS 応答を受け取ります。
6. サード・パーティー・ソリューションに実装する必要がある情報を確認し、収集します。

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。

カスタム・アクション

ネットワーク・イベントに対する応答としてカスタム・アクションを実行するスクリプトをカスタム・ルールに追加できます。「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・アクションにより、スクリプトおよび実行されるアクションに渡す値を選択または定義できます。

例えば、ログイン試行の失敗回数を定義し、それによってトリガーされるルールへの応答として、ご使用のネットワークからあるソース IP アドレスをブロックするファイアウォール・ルールを作成するスクリプトを作成できます。

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。

注**:** この機能は、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。

「カスタム・アクション」ウィンドウのツールバーで「追加」をクリックして、「カスタム・アクションの定義」ダイアログを開きます。このダイアログで、カスタム・アクションを定義するスクリプトをアップロードできます。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。

注**:** 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。

アップロードするスクリプトに渡すパラメーターとして、以下の 2 種類のパラメーターを定義できます。

表 6. 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	固定プロパティーは、カスタム・アクション・スクリプトに渡される値です。 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である *username* と *password* をスクリプトに渡して、SMS アラートの送信などの定義済みアクションを実行できます。 「暗号化値」チェック・ボックスを選択することで、パスワードなどの固定プロパティーを暗号化できます。
ネットワーク・イベント・プロパティー	ネットワーク・イベント・プロパティーは、イベントによって生成される動的な Ariel プロパティーです。スクリプトに渡すネットワーク・イベント・プロパティーを「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るかをテストできます。スクリプトをテストするには、カスタム・アクションを選択して、「テストの実行」 > 「実行」をクリックします。「カスタム・アクション実行のテスト」ダイアログに、テストの結果と、スクリプトによって生成された出力が返されます。

カスタム・アクション・スクリプトは、QRadar 管理対象ホスト上のサンドボックス環境内で実行されます。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。カスタム・アクション・スクリプトは、ルールを起動したイベント・プロセッサーを実行する管理対象ホスト上で実行されます。

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 SIEM* ユーザーズ・ガイド」を参照してください。

第 3 章 ユーザー管理

管理者は、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。初期構成後は、ユーザー・アカウントを編集して、ユーザー情報を最新の状態にすることができます。必要に応じて、ユーザー・アカウントの追加と削除を行うこともできます。

ユーザー管理の概要

ユーザー・アカウントは、ユーザー名、ユーザーのデフォルトのパスワード、ユーザーの E メール・アドレスを定義します。

作成した新しいユーザー・アカウントごとに、以下の項目を割り当てます。

- ユーザー・ロール - QRadar の機能と情報にアクセスするための、ユーザーに付与される特権を決定します。デフォルトのユーザー・ロールとして、「管理」と「すべて」の 2 つが定義されています。ユーザー・アカウントを追加する前に、ユーザーの特定の権限要件を満たすために、追加のユーザー・ロールを作成する必要があります。
- セキュリティー・プロファイル - ユーザーにアクセスを許可するネットワーク、ログ・ソース、およびドメインを決定します。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。この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。

ロールの管理

「ユーザー・ロール」ウィンドウを使用して、ユーザー・ロールの作成と管理を行うことができます。

ユーザー・ロールの作成

このタスクを実行して、デプロイメントに必要となるユーザー・ロールを作成します。

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 SIEM 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. 以下のパラメーターを構成します。
   a. 「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。
   b. このユーザー・ロールに割り当てる権限を選択します。 37 ページの『ユーザー・ロールのアクセスと権限』を参照してください。
6. 「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**:**

   a. 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。
   b. 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。
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。 37 ページの『ユーザー・ロールのアクセスと権限』を参照してください。
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・プロファイルの管理

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。

「セキュリティー・プロファイル管理」ウィンドウを使用して、セキュリティー・プロファイルの表示、作成、更新、削除を行うことができます。

権限の優先順位

このトピックでは、権限の優先順位の各オプションを定義します。

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。

以下の制限を理解しておくようにしてください。

- 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と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。
- ネットワークおよびログ・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。

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

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。この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。
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。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、 17 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、 17 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・アカウント管理

このトピックでは、ユーザー・アカウントの管理について説明します。

ご使用のシステムを初めて構成する場合は、ユーザーごとにユーザー・アカウントを作成する必要があります。初期構成後に、追加のユーザー・アカウントの作成や、既存のユーザー・アカウントの管理が必要になる場合があります。

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. 次の各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、以下の基準を満たしている必要があります。
      - 5 文字以上であること。
      - 255 文字以内であること。
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・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。

認証管理

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した場合、そのユーザーがもう一度システムにアクセスするには、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。認証のためのコンソール設定の構成について詳しくは、 61 ページの『QRadar システム時刻の構成』を参照してください。

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、 75 ページの『第 6 章 QRadarのセットアップ』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。

管理ユーザーの外部認証

管理ユーザーは、外部認証が失敗した場合でも IBM Security QRadar にログインできる必要があります。

外部認証が構成されている場合は、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。ユーザーがログインすると、まずユーザー名とパスワードがリモート認証局に対して検証されます。リモート認証局が使用可能でない場合は、パスワードがローカルに検証され、ユーザーはログインして管理機能を実行できます。

ローカル・パスワードはリモート認証局と同期されません。リモート認証局が使用不可の場合に QRadar にログインできなくなることがないように、リモート認証局のパスワードを更新する際は必ずローカル・パスワードを同時に更新してください。

リモート認証局がアクティブであるときは、ローカル管理パスワードを変更できません。管理パスワードを変更するには、外部認証を一時的に無効にしてパスワードをリセットし、外部認証を再構成する必要があります。

非管理ユーザーを作成する場合は、ローカル・パスワードが設定されません。非管理ユーザーの認証は、リモート認証局に対してのみ行われます。リモート認証局が使用不可の場合、またはユーザー資格情報が拒否された場合、ユーザーはログインできません。

システム認証の構成

QRadar システムでローカル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、「システム認証」を選択します。
5. 「保存」をクリックします。

RADIUS 認証の構成

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、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

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。
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 (LDAP Context)	使用する LDAP コンテキストを入力します (例: DC=QRADAR,DC=INC)。

パラメーター	説明
LDAP ドメイン	使用するドメインを入力します (例: qradar.inc)。

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、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 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、 34 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 *7. 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。
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。

表 *7. LDAP* 基本構成パラメーター *(*続き*)*

パラメーター	説明
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 *8. 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 *9. 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」タブで、「システム構成」をクリックし、次に「認証」をクリックします。
2. 「認証モジュール」リストで「**LDAP**」を選択します。

3. 「同期の管理」をクリックし、次に「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. LDAP ユーザー・パスワードを暗号化するには、/opt/qradar/bin/runjava.sh com.q1labs.core.util.PasswordEncrypt [*password*] スクリプトを実行します。

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 IBM Security 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。

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 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 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 *10.* 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
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 11. 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

ユーザー・ロールのアクセスと権限

IBM Security QRadar の機能へのアクセスを制限するには、「ユーザー・ロール管理」ウィンドウのパラメーターを使用します。

以下の表では、「ユーザー・ロール管理」ウィンドウのパラメーターについて説明します。「ユーザー・ロール管理」ウィンドウに表示されるパラメーターは、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 12. 「ユーザー・ロール管理」ウィンドウのパラメーターの説明

パラメーター	説明
ユーザー・ロール名	ロールの固有の名前。
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。以下に示す特定の管理アクセス権を付与できます。 管理者の管理者 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。特定の管理アクセス権を付与します。 リモート・ネットワークおよびサービス構成 「管理」タブでリモート・ネットワークとサービスを構成するための権限を付与します。 システム管理者 ユーザー・インターフェースの全領域にアクセスするための権限を付与します。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。

表 12. 「ユーザー・ロール管理」ウィンドウのパラメーターの説明 (続き)

パラメーター	説明
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。以下に示す特定の権限を付与できます。 オフェンスをユーザーに割り当て 他のユーザーにオフェンスを割り当てるための権限を付与します。 カスタム・ルールの保守 カスタム・ルールを作成および編集するための権限を付与します。 オフェンスのクローズ理由の管理 オフェンスのクローズ理由を管理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。
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。カスタムのイベント・プロパティーについて詳しくは、「ユーザーズ・ガイド」を参照してください。 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 12. 「ユーザー・ロール管理」ウィンドウのパラメーターの説明 (続き)

パラメーター	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*」ガイド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 12. 「ユーザー・ロール管理」ウィンドウのパラメーターの説明 (続き)

パラメーター	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対するアクセス権限を付与します。以下に示すユーザー固有の権限を付与できます。 **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。IBM Security 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 User Guide*」を参照してください。

表 12. 「ユーザー・ロール管理」ウィンドウのパラメーターの説明 (続き)

パラメーター	説明
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。

セキュリティー・プロファイルのパラメーター

以下の表で、「セキュリティー・プロファイル管理」ウィンドウのパラメーターについて説明します。

表 13. 「セキュリティー・プロファイル管理」ウィンドウのパラメーター

パラメーター	説明
セキュリティー・プロファイル名	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。
説明	**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。

「ユーザー管理」ウィンドウのパラメーター

以下の表で、「ユーザー管理」ウィンドウのパラメーターについて説明します。

表 *14.* 「ユーザー管理」ウィンドウのパラメーター

パラメーター	説明
ユーザー名	このユーザー・アカウントのユーザー名を表示します。
説明	このユーザー・アカウントの説明を表示します。
E メール	このユーザー・アカウントの E メール・アドレスを表示します。
ユーザー・ロール	このユーザー・アカウントに割り当てられているユーザー・ロールを表示します。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	このユーザー・アカウントに割り当てられているセキュリティー・プロファイルを表示します。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。

「ユーザー管理」ウィンドウのツールバー

「ユーザー管理」ウィンドウのツールバー機能

以下の表で、「ユーザー管理」ウィンドウのツールバー機能について説明します。

表 *15.* 「ユーザー管理」ウィンドウのツールバー機能

機能	説明
新規	ユーザー・アカウントを作成するには、このアイコンをクリックします。ユーザー・アカウントを作成する方法について詳しくは、23 ページの『ユーザー・アカウントの作成』を参照してください。
編集	選択したユーザー・アカウントを編集するには、このアイコンをクリックします。
削除	選択したユーザー・アカウントを削除するには、このアイコンをクリックします。
ユーザーの検索 (Search Users)	このテキスト・ボックスにキーワードを入力して Enter を押すと、特定のユーザー・アカウントを見つけることができます。

「ユーザー詳細 (User Details)」ウィンドウのパラメーター

「ユーザー詳細 (User Details)」ウィンドウのパラメーター

以下の表で、「ユーザー詳細 (User Details)」ウィンドウのパラメーターについて説明します。

表 16. 「ユーザー詳細 (User Details)」ウィンドウのパラメーター

パラメーター	説明
ユーザー名	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。
E メール	ユーザーの E メール・アドレス。E メール・アドレスは、以下の要件を満たしている必要があります。 • 有効な E メール・アドレスであること。 • 10 文字以上であること。 • 255 文字以内であること。
パスワード	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、以下の基準を満たしている必要があります。 • 5 文字以上であること。 • 255 文字以内であること。
パスワードの確認	確認のため、パスワードを再度入力します。
説明	**オプション。**ユーザー・アカウントの説明を入力します。最大 2,048 文字まで入力できます。
ユーザー・ロール	リスト・ボックスから、このユーザーに割り当てるユーザー・ロールを選択します。 ユーザー・ロールの追加、編集、削除を行うには、「ユーザー・ロールの管理 **(Manage User Roles)**」リンクをクリックします。ユーザー・ロールについて詳しくは、 15 ページの『ロールの管理』を参照してください。
セキュリティー・プロファイル	このユーザーに割り当てるセキュリティー・プロファイルをリスト・ボックスから選択します。 セキュリティー・プロファイルの追加、編集、削除を行うには、「セキュリティー・プロファイルの管理」リンクをクリックします。セキュリティー・プロファイルについて詳しくは、 17 ページの『セキュリティー・プロファイルの管理』を参照してください。

第 4 章 システムおよびライセンス管理

QRadar デプロイメント内のシステムとライセンスを管理します。

デプロイメント内の各システム (ソフトウェア・アプライアンスを含む) にライセンスを割り振る必要があります。QFlow および QRadar Event Collectorは、ライセンスを必要としません。

QRadar システムをインストールすると、デフォルトのライセンス・キーを使用して、ユーザー・インターフェースに 5 週間アクセスすることができます。デフォルトのライセンスの有効期限が切れる前に、ライセンス・キーをシステムに割り振る必要があります。ライセンスを追加して、QRadar Vulnerability Manager などの QRadar 製品を有効にすることもできます。

ライセンスの再割り振りには 14 日間の猶予期間があります。ライセンス・キーがアップロードされている場合、ホストにフィックスが適用された後またはアンロック・キーがアップロードされた後に、ライセンスをアンロックすることができます。この猶予期間が経過すると、ライセンスはシステムにロックされます。

ライセンス状況が「無効」の場合、ライセンスを取り換える必要があります。この状況の場合、ライセンスが許可なく変更された可能性があります。

ライセンスの変更をデプロイするまで、ライセンスはデプロイされません。

システムおよびライセンス管理の概要

「システムおよびライセンス管理」ウィンドウでは、システムとライセンス・キーの管理、およびシステムの再始動とシャットダウンを行います。

「システムおよびライセンス管理」ウィンドウのツールバーには、以下の機能が組み込まれています。

表 *17.* 「システムおよびライセンス管理」ウィンドウのツールバーの機能

機能	説明
システムへのライセンスの割り振り	この機能を使用して、システムにライセンスを割り振ります。 「表示」メニューで「ライセンス」を選択すると、この機能のラベルが「ライセンスへのシステムの割り振り」に変わります。
ライセンスのアップロード	この機能を使用して、コンソールにライセンスをアップロードします。詳しくは、 48 ページの『ライセンス・キーのアップロード』を参照してください。

表 17. 「システムおよびライセンス管理」ウィンドウのツールバーの機能 (続き)

機能	説明
アクション (ライセンス)	「表示」メニューの「ライセンス」を選択して、ライセンス・メニュー・オプションを表示します。 デプロイされたライセンスに対して、割り振りの猶予期間内 (デプロイメント後 14 日間以内) に「アクション」 > 「割り振りを元に戻す」を選択すると、ライセンスの状態が「アンロック済み」に変わります。アンロック済みのライセンスは、別のシステムに再割り振りできます。
アクション (システム)	「表示」メニューの「システム」を選択し、「アクション」メニューをクリックして以下のオプションを表示します。 システムの表示と管理 - システムを選択してから、「アクション」 > 「システムの表示と管理」をクリックして「システム情報」ウィンドウを表示します。「ライセンス」、「ファイアウォール」、「ネットワーク・インターフェース」、「**E** メール・サーバー」の各タブをクリックして、使用するシステムのこれらのエレメントを構成します。 **HA** ホストの追加 **(Add HA Host)** - システムを選択してからこのオプションを選択すると、HA ホストがシステムに追加され、HA クラスターが生成されます。HA について詳しくは、製品の「高可用性ガイド」を参照してください。 割り振りを元に戻す - このオプションを選択すると、ステージング済みライセンスの変更が取り消されます。構成は、最後にデプロイされたライセンスの割り振りに戻ります。 **注:** デプロイされたライセンスに対して、割り振りの猶予期間内 (デプロイメント後 14 日間以内) に割り振りを元に戻すと、ライセンスの状態が「アンロック済み」に変わります。「アンロック済み」のライセンスは、別のシステムに再割り振りできます。 **Web** サーバーの再始動 - このオプションを選択すると (必要な場合)、ユーザー・インターフェースが再始動します。例えば、新しいユーザー・インターフェース・コンポーネントが追加された新しいプロトコルをインストールした場合は、ユーザー・インターフェースの再始動が必要になることがあります。 システムのシャットダウン - システムを選択してからこのオプションを選択すると、そのシステムがシャットダウンされます。詳しくは、 54 ページの『システムのシャットダウン』を参照してください。 システムの再始動 - システムを選択してからこのオプションを選択すると、そのシステムが再始動します。詳しくは、 54 ページの『システムの再始動』を参照してください。 ログ・ファイルの収集 - 選択したホストのログ・ファイルを収集します。

「表示」メニューから「ライセンス」を選択すると、「システムおよびライセンス管理」ウィンドウに以下の情報が表示されます。

表 *18.* 「システムおよびライセンス管理」ウィンドウのパラメーター - 「ライセンス」ビュー

パラメーター	説明
ホスト名	このライセンスに割り振られているシステム。
ホスト **IP**	このライセンスに割り振られているシステム。
ライセンス・アプライアンス・タイプ	このライセンスに割り振られているアプライアンスのタイプ。
ライセンス・アイデンティティー	このライセンスが提供する IBM Security QRadar 製品の名前。
ライセンスの状況	当該システムに割り振られているライセンスの状況は、以下のいずれかです。 未割り振り - ライセンスはシステムに割り振られていません。 未デプロイ - ライセンスはシステムに割り振られていますが、割り振りの変更がデプロイされていません。この場合、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。 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。 アンロック済み - ライセンスはロック解除されています。過去 10 日以内にデプロイされたライセンスはアンロックできます。これは、ライセンスを再割り振りするためのデフォルトの猶予期間です。この猶予期間が経過すると、ライセンスはシステムにロックされます。この期間の経過後にライセンスのロックを解除する必要がある場合は、カスタマー・サポートにお問い合わせください。 無効 - ライセンスは無効で、置き換える必要があります。この状況の場合、ライセンスが許可なく変更された可能性があります。
ライセンスの有効期限	有効期限の日付。
イベント速度制限	ライセンス条項に従って許可される最大イベント速度。
フロー速度制限	ライセンス条項に従って許可される最大フロー速度。

ライセンス管理のチェックリスト

「システムおよびライセンス管理」ウィンドウで選択可能なオプションを使用して、ライセンス・キーを管理します。

デフォルトのライセンス・キーでは、ユーザー・インターフェースへのアクセスを 5 週間提供します。ライセンス・キーをシステムに割り振る必要があります。

ユーザーがツールを使用するためには、QRadar システムをセットアップする必要があります。まずライセンス・キーを取得してください。ライセンス・キーを取得したら、ライセンス・キーをコンソールにアップロードし、システムに割り振る必要があります。

システムの初期セットアップ時には、以下のタスクを実行する必要があります。

手順

1. 以下のいずれかの方法で、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。
   - 他のすべての技術的な問題については、カスタマー・サポート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。

   ライセンス・キーをアップロードすると、「システムおよびライセンス管理」ウィンドウにリストされますが、この時点ではまだ割り振られていません。詳しくは、『ライセンス・キーのアップロード』を参照してください。
3. 取得したライセンスをシステムに割り振るか、またはシステムをライセンスに割り振ります。
4. 変更をデプロイするには、「管理」タブのメニューから、「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。

ライセンス・キーのアップロード

新規 QRadar システムのインストール、有効期限が切れたライセンスの更新、またはデプロイメント環境への QRadar 製品 (QRadar Vulnerability Manager など) の追加を行う場合は、ライセンス・キーを QRadar コンソールにアップロードします。

始める前に

ライセンス・キーに関するサポートが必要な場合は、以下にお問い合わせください。

- 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。
- 他のすべての技術的な問題については、カスタマー・サポートにお問い合わせください。

このタスクについて

QRadar コンソールにログオンしたときにライセンス・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・システムのいずれかでライセンス・キーの有効期限が切れている場合は、ログイン時に、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。ライセンス・キーを更新するには、「システムおよびライセンス管理」ウィンドウにアクセス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・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. 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。
5. 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。
6. 「ファイルのアップロード (File Upload)」ウィンドウで、ライセンス・キーを探して選択します。
7. 「オープン」をクリックします。
8. 「アップロード」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、ライセンスは割り振られません。

次のタスク

53 ページの『ライセンスのシステムへの割り振り』

ライセンスのシステムへの割り振り

「システムおよびライセンス管理」ウィンドウからライセンスを割り振ります。

このタスクについて

QRadar システムをインストールすると、デフォルトのライセンス・キーを使用して、ユーザー・インターフェースに 5 週間アクセスすることができます。デフォルトのライセンスの有効期限が切れる前に、ライセンス・キーをシステムに割り振る必要があります。ライセンスを追加して、QRadar Vulnerability Manager などの QRadar 製品を有効にすることもできます。

複数のライセンスを 1 つのシステムに割り振ることができます。例えば、IBM Security QRadar SIEM のほかに、IBM Security QRadar Risk Manager と IBM Security QRadar Vulnerability Manager を QRadar コンソール・システムに割り振ることができます。

、QRadar システムのライセンスの状況には、以下のものがあります。

- 未割り振り - ライセンスはシステムに割り振られていません。
- 未デプロイ - ライセンスはシステムに割り振られていますが、割り振りの変更がデプロイされていません。この場合、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。
- 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。
- アンロック済み - 過去 10 日以内にデプロイされたライセンスはアンロックできます。これは、ライセンスを再割り振りするためのデフォルトの猶予期間です。この猶予期間が経過すると、ライセンスはシステムにロックされます。この期間の経過後にライセンスのロックを解除する必要がある場合は、カスタマー・サポートにお問い合わせください。
- 無効 - ライセンスは無効で、置き換える必要があります。この状況の場合、ライセンスが許可なく変更された可能性があります。

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」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、「ライセンス」を選択します。
5. まだ割り振られていないライセンスを選択します。
6. 「ライセンスへのシステムの割り振り」をクリックします。
7. オプション: ライセンスのリストをフィルタリングするには、「ライセンスのアップロード」検索ボックスにキーワードを入力します。
8. ライセンスのリストからライセンスを選択します。
9. システムを選択します。
10. 「システムへのライセンスの割り振り」をクリックします。

割り振りを元に戻す

割り振られたライセンスを、14 日間の猶予期間内に元に戻すことができます。

このタスクについて

ライセンスをシステムに割り振った場合でも、構成の変更をデプロイする前であれば、ライセンスの割り振りを取り消すことができます。ライセンスの割り振りを取り消しても、最後にシステムに割り振られてデプロイされたライセンスは維持されます。

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、「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、「ライセンス」を選択します。
5. 元に戻したいライセンスを選択します。
6. 「アクション」 > 「割り振りを元に戻す」をクリックします。

ライセンスの詳細の表示

ライセンス・キーは、情報を提供するとともに、IBM Security QRadar システムで制限と機能を適用します。

このタスクについて

「システムおよびライセンス管理」ウィンドウで、ライセンスの詳細 (許可されるログ・ソースの数や有効期限など) を表示することができます。

注: 構成されているログ・ソースの制限を超過すると、エラー・メッセージが表示されます。ログ・ソースが自動ディスカバーされて制限を超過している場合、それらのログ・ソースは自動的に無効になります。ログ・ソースの数を拡張する場合は、営業担当員にお問い合わせください。

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」メニューから、「ライセンス」を選択します。
5. ホストのライセンス情報を表示するには、ホストを選択し、「アクション」 > 「ライセンスの表示」をクリックします。

次のタスク

「ライセンス」ウィンドウでは、以下のタスクを実行することができます。

- 「ライセンスのアップロード」をクリックしてライセンスをアップロードする。ライセンス・キーのアップロードを参照してください。
- ツールバーの「システムへのライセンスの割り振り」をクリックしてライセンスを割り当てる。 システムへのライセンスの割り振りを参照してください。

ライセンスのエクスポート

デスクトップ・システムの外部ファイルにライセンス・キーの情報をエクスポートします。

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. 「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、「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. 以下のいずれかのオプションを選択します。

   アプリケーションから開く **(Open with)**
   : 選択したアプリケーションを使用して、ライセンス・キー・データを開きます。

   ファイルの保存 **(Save File)**
   : ファイルをデスクトップに保存します。

7. 「**OK**」をクリックします。

システム管理

「システムおよびライセンス管理」ウィンドウを使用して、デプロイメント環境内のシステムを管理します。

システム情報の表示、ライセンスの管理、システムの管理、システムの再始動とシャットダウン、HA ホストの追加、およびログ・ファイルの収集を行い、システムでその他の管理アクティビティーを実行します。

システムおよびライセンスの詳細の表示

システムについての情報 (ライセンスを含む) を「システムの詳細」ウィンドウで表示します。

このタスクについて

システムに関する情報とシステムに割り振られているライセンスを表示するには、「システムの詳細」ウィンドウを開きます。

「ライセンス」ペインには、選択したシステムに割り振られている各ライセンスについて、以下の詳細が表示されます。

表 *19.* ライセンスのパラメーター

パラメーター	説明
ライセンス・アイデンティティー	このライセンスが提供する IBM Security QRadar 製品の名前。
ライセンスの状況	当該システムに割り振られているライセンスの状況は、以下のいずれかです。 未割り振り - ライセンスはシステムに割り振られていません。 未デプロイ - ライセンスはシステムに割り振られていますが、割り振りの変更がデプロイされていません。この場合、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。 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。 アンロック済み - ライセンスはロック解除されています。過去 10 日以内にデプロイされたライセンスはアンロックできます。これは、ライセンスを再割り振りするためのデフォルトの猶予期間です。この猶予期間が経過すると、ライセンスはシステムにロックされます。この期間の経過後にライセンスのロックを解除する必要がある場合は、カスタマー・サポートにお問い合わせください。 無効 - ライセンスは無効で、置き換える必要があります。この状況の場合、ライセンスが許可なく変更された可能性があります。
ライセンス・アプライアンス・タイプ **(License Appliance Types)**	このライセンスに割り振られているアプライアンスのタイプ。
ライセンスの有効期限	有効期限の日付。
イベント速度制限	ライセンス条項に従って許可される最大イベント速度。

表 19. ライセンスのパラメーター (続き)

パラメーター	説明
フロー速度制限	ライセンス条項に従って許可される最大フロー速度。

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」を選択します。
5. システムの詳細を表示するために、ホストを選択して「アクション」 > 「システムの表示と管理」をクリックするか、ホストをダブルクリックします。
6. 「ライセンス」タブをクリックします。

次のタスク

「ライセンス」ペインでは、以下のタスクを実行することができます。

- ライセンスを選択して「ライセンスの表示 **(View License)**」をクリックします。 50 ページの『ライセンスの詳細の表示』を参照してください。
- 「ライセンスのアップロード」をクリックします。 48 ページの『ライセンス・キーのアップロード』を参照してください。
- ツールバーの「システムへのライセンスの割り振り」をクリックしてライセンスを割り当てる。 システムへのライセンスの割り振りを参照してください。

システム・ヘルス

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。

「管理」タブの「システム構成」領域で、「管理」 > 「システム構成」 > 「システムの正常性」アイコンを選択すると、CPU 使用状況、ネットワーク読み取り/書き込み、ディスク読み取り/書き込み、メモリー使用状況、フロー/秒 (FPS)、およびイベント/秒 (EPS) が表示されます。

マウスをグラフ上に移動すると、詳細情報とグラフ化されているメトリックが表示されます。

ライセンスのシステムへの割り振り

ライセンスを取得してアップロードしてから、「システムおよびライセンス管理」ウィンドウのメニューを使用してライセンスを割り振ります。

複数のライセンスを 1 つのシステムに割り振ることができます。例えば、IBM Security QRadar SIEM のほかに、IBM Security QRadar Risk Manager と IBM Security QRadar Vulnerability Manager を QRadar コンソール・システムに割り振ることができます。

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」を選択します。
5. 使用可能なシステムを選択します。
6. 「システムへのライセンスの割り振り」をクリックします。
7. オプション: ライセンスのリストをフィルタリングするには、「ライセンスのアップロード」検索ボックスにキーワードを入力します。
8. ライセンスのリストからライセンスを選択します。
9. システムを選択します。
10. 「システムへのライセンスの割り振り」をクリックします。

システムの再始動

「システムおよびライセンス管理」ウィンドウの「アクション」メニューから、デプロイメント環境内のシステムを再始動することができます。

このタスクについて

データ収集は、システムのシャットダウン中および再始動中は停止します。

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. 「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」を選択します。
5. 再始動するシステムを選択します。
6. 「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。

システムのシャットダウン

「システムおよびライセンス管理」ウィンドウの「アクション」メニューから、デプロイメント環境内のシステムをシャットダウンすることができます。

このタスクについて

システムのシャットダウン中は、データ収集処理は停止します。

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. 「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」を選択します。
5. シャットダウンするシステムを選択します。
6. 「アクション」メニューから、「シャットダウン」を選択します。

システムの詳細のエクスポート

「システムおよびライセンス管理」ウィンドウの「アクション」メニューから、システム情報を外部ファイルにエクスポート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」を選択します。
5. 「アクション」メニューから、「システムのエクスポート **(Export Systems)**」を選択します。
6. 以下のいずれかのオプションを選択します。

   アプリケーションから開く **(Open with)**
   選択したアプリケーションを使用して、ライセンス・キーを開きます。

   ファイルの保存 **(Save File)**
   ファイルをデスクトップに保存します。
7. 「**OK**」をクリックします。

ログ・ファイルの収集

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。ログ・ファイルの収集に要する時間は、デプロイメントのサイズと、ログ・ファイル収集対象に組み込むホストの数に応じて異なります。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する必要があります。

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」タブをクリックします。
2. ナビゲーション・ウィンドウで「システム構成」をクリックし、「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。
3. キーボードで Ctrl キーを押しながら、ログ・ファイル収集に含める各ホストをクリックします。
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 **(Advanced Options)**」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。
7. 「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。

   アクティブなログ・ファイル収集プロセスをキャンセルするには、通知メッセージの「**X**」をクリックします。
8. ログ・ファイル収集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」という通知の「ここをクリックしてファイルをダウンロードします」をクリックします。

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 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 *20.* **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。

表 20. **check_ariel_integrity.sh** ユーティリティーのパラメーター (続き)

パラメーター	説明
-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。

管理対象ホストの帯域幅に関する考慮事項

ご使用の IBM Security QRadar デプロイメント内の管理対象ホストの帯域幅使用量について検討します。

状態および構成データを複製するには、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。システムとネットワークのパフォーマンスは、データの検索速度に影響します。ストア・アンド・フォワード構成を備えた QRadar イベント・コレクターは、すべてのデータをスケジュールに基づいて転送します。必ず、収集を予定している

データに対して十分な帯域幅を割り振ってください。そうしないと、ご使用のストア・アンド・フォワード・アプライアンスが、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
: データを収集しているときに、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長期検索を実行しない
: 帯域幅が制限されているリンク上でユーザーが長期検索を実行しないようにしてください。正確なフィルターを使用して検索を行うと、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、結果のデータを送り返すために必要な帯域幅の量が削減されます。

インストール後の管理対象ホストおよびコンポーネントのデプロイ

インストール後に、管理対象ホストをデプロイメント環境に追加することができます。分散処理を支援するため、QRadar Event Collector、QRadar フロー・プロセッサー、または他のアプライアンスをデプロイメント環境に追加することができます。

このタスクについて

管理対象ホスト上では、脆弱性スキャナーなどのコンポーネントを構成できます。

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 User Guide*」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」タブをクリックします。
2. 「システム構成」ペインで、「システムおよびライセンス管理」をクリックします。

3. ホストの表から、管理する以下のアプライアンスのいずれかを選択します。
   - QRadar コンソール
   - QRadar 管理対象ホスト
4. オプション: ソフトウェア・インストールのコンポーネントを追加および構成するには、「デプロイメント・アクション」メニューを使用します。「デプロイメント・アクション」 > 「デプロイメントの表示」を選択すると、デプロイメント環境の視覚図が表示されます。

   「デプロイメント・ビュー」ウィンドウで、デプロイメント環境を視覚化した 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。
5. 「デプロイメント・アクション」メニューからアクションを選択します。
6. 必要な情報を入力して、該当するオプションを選択します。
7. 「システムおよびライセンス管理」ウィンドウを閉じます。
8. 「管理」タブをクリックします。
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。

システム情報の構成

QRadar セキュリティー・システムを稼働させたり、システムの保守を行うために、「システム情報」ウィンドウから QRadar コンソールと管理対象ホストのシステム設定を構成する必要があります。

このタスクについて

ネットワーク・インターフェースへのロールの割り当て、ライセンスの管理、QRadar で使用する E メール・サーバーの構成、およびローカル・ファイアウォールを使用した外部デバイスから QRadar へのアクセスの管理を行うことができます。

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) を行う必要がある場合は、**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。

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。

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」を選択します。
5. 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。
6. 「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。

注: 選択したホストを右クリックするとこのメニュー・オプションにアクセスできます。またはホストをダブルクリックして「システム情報」ウィンドウを開くことができます。

7. QRadar デプロイメント外部の指定デバイスからこのホストへのアクセスを許可するためにローカル・ファイアウォールを構成するには、「ファイアウォール」タブをクリックします。
   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. 矢印をクリックしてこのアクセス・ルールを追加します。
8. QRadar システムのネットワーク・インターフェースを構成するには、「ネットワーク・インターフェース」タブをクリックします。
   a. 「デバイス」列でネットワーク・インターフェースを選択します。
   b. 「編集」をクリックします。
   c. パラメーターを構成します。

   管理、HA クロスオーバー、またはスレーブのロールが割り当てられたネットワーク・インターフェースは編集できません。
9. アラート、レポート、通知、およびイベント・メッセージを配信するための E メール・サーバーを構成するには、「**E** メール・サーバー」タブをクリックします。
   a. 「**E** メール・サーバー・アドレス」フィールドに、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。

      E メール・サーバーがない場合に、QRadar が提供する E メール・サーバーを使用するときは、ローカル E メール処理を実施するために `localhost` と入力します。

      QRadar の設定中に、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。例えば、*You@YourCompany.com* にメールを送信する場合、*YourCompany.com* への到達方法を把握しているメール・リレー・サーバーを「**E** メール・サーバー」設定に構成する必要があります。

      メール・サーバー設定を `localhost` として構成した場合、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。 外部にメールを配信する場合は、有効なメール・リレー・サーバーを使用してください。

      注: E メール・サーバー接続にはポート 25 を使用することが推奨されます。
10. 「保存」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。

QRadar システム時刻の構成

複数のタイム・ゾーンにまたがるシステムを実行する場合は、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、グリニッジ標準時 (GMT) を使用するようにすべてのアプライアンス (QRadar コンソールを含む) を構成することもできます。

以下のいずれかの方法を使用して、IBM Security QRadar システム時刻を構成します。

- システム時刻を保持するように Network Time Protocol (NTP) サーバーを構成します。

  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。
- システム時刻を手動で構成します。

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。

IBM Security QRadar SIEM Console でのシステム時刻の手動構成

QRadar コンソール上でシステム時刻 を手動で設定し、この時刻を管理対象ホストと同期します。

このタスクについて

システム時刻を手動で調整する前に QRadar サービスを停止してから、**date** コマンドを使用してシステム時刻と日付を変更します。

手順

1. QRadar サービスを停止します。

   ```
   service hostcontext stop

   service tomcat stop

   service hostservices stop
   ```

2. **date** コマンドを時刻パラメーターとともに入力します。

   date <*MMddhhmm*><YYYY>

   例えば、時刻を 2018 年 12 月 13 日午後 5:24 に設定する場合は、以下のコマンドを入力します。

   ```
   date 121317242018
   ```

3. システム・ハードウェア・クロックを現在時刻に同期します。

   ```
   /sbin/hwclock --systohc
   ```

4. QRadar サービスを再始動します。

   ```
   service hostservices start

   service tomcat start

   service hostcontext start
   ```

5. 以下のコマンドを入力して、QRadar コンソールの時刻を QRadar 管理対象ホストと同期します。

   ```
   /opt/qradar/support/all_servers.sh /opt/qradar/bin/time_sync.sh
   ```

6. 「管理」タブで「拡張」 > 「すべての構成のデプロイ」をクリックして、すべての QRadar 管理対象ホストでサービスを再始動します。

   これで、QRadar コンソールと管理対象ホストの間で時刻が同期されました。

   QRadar コンソールの時刻をタイム・サーバーと同期するには、QRadar コンソールで時刻同期サービスを有効にする必要があります。

IBM Security QRadar SIEM Console でのタイム・サーバーの構成

QRadar コンソールで時刻同期サービスを有効にして、管理対象ホスト全体で時刻を同期します。

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. ntp.conf ファイルを編集します。

   ```
   vi /etc/ntp.conf
   ```

3. ntp.conf ファイルの server セクションで、既存のサーバー項目をそのままにするか、独自の内部 NTP (Network Time Protocol) サーバーで置き換えます。 ntp.conf ファイルのサーバー項目は、「server」で始まります。

   NTP プロジェクト (http://www.ntp.org/) のパブリック・サーバーを使用することができます。

   ```
   server 0.rhel.pool.ntp.org iburst
   server 1.rhel.pool.ntp.org iburst
   server 2.rhel.pool.ntp.org iburst
   server 3.rhel.pool.ntp.org iburst
   ```

   パブリック NTP サーバーを使用する場合は、使用するファイアウォールがアウトバウンド NTP 要求を許可していることを確認します。
4. 変更を保存し、ファイルを閉じます。
5. ntpd サービスを有効にして実行レベル 3 で実行できるようにします。

   ```
   chkconfig --level 3 ntpd on
   ```

6. ntpd サービスが再始動時に有効になって実行されることを確認します。

   ```
   chkconfig --list ntpd
   ```

   出力に 3:on が表示されることを確認します。

   ```
   ntpd 0:off 1:off 2:off 3:on 4:off 5:off 6:off
   ```

7. システム時刻を変更する際にデータ収集エラーが発生するのを防ぐために、QRadar サービスを停止します。

   ```
   service hostcontext stop

   service tomcat stop

   service hostservices stop
   ```

8. NTP サーバーと時刻を同期します。

   ```
   ntpdate <ntp.server.address>
   ```

9. ntpd サービスを始動します。

   ```
   service ntpd start
   ```

10. QRadar サービスを再始動します。

    ```
    service hostservices start

    service tomcat start

    service hostcontext start
    ```

11. 以下のコマンドを入力して、すべての管理対象ホストの時刻を QRadar コンソールと同期します。

    ```
    /opt/qradar/support/all_servers.sh /opt/qradar/bin/time_sync.sh
    ```

12. 「管理」タブで「拡張」 > 「すべての構成のデプロイ」をクリックして、すべての QRadar 管理対象ホストでサービスを再始動します。

    これで、QRadar コンソールと管理対象ホストの間で時刻が同期されました。

第 5 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。

IBM Security QRadar SIEM 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。

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 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 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。

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 21. 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。

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`
- `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。 71 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、「ユーザーズ・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、「ユーザーズ・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。 71 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。 74 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

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。必要な場合は、自己署名証明書の作成とインポートも行ってください。

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 22. 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 22. 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. ご使用のシステムを Tivoli Directory Integrator 対して認証するために証明書ベースの認証が必要な場合は、以下のいずれかの処理を行います。

- 自己署名証明書を作成してインポートする場合は、ステップ 7 に進みます。
- CA 証明書をインポートする場合は、ステップ 8 に進みます。

7. 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。
8. 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。
9. <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現行パスワードが、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。

10. Tivoli Directory Integrator を始動するには、以下のいずれかのスクリプトを使用します。
    - QradarIAM.sh (Linux の場合)
    - QradarIAM.bat (Microsoft Windows の場合)

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、 68 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 23. 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	QRadar SIEM 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。

表 23. 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
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。
search filter	Identity and Access Management レジストリーから取得されたユーザー情報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、 71 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、71 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、66 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 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。

ネットワーク階層

QRadar は、ネットワーク階層を使用してネットワーク・トラフィックを理解し、デプロイメント全体のアクティビティーを確認するための機能を提供します。

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。

ネットワーク階層を定義する際、グループ化が可能なシステム、ユーザー、およびサーバーを考慮する必要があります。

振る舞いが類似しているシステムおよびユーザー・グループはグループ化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。特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、具体的なポリシーを管理できるようになります。

グループ内では、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できます。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。

デプロイメントで 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できます。

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・パターン別に編成できます。例えば、メール・サーバー・グループ、部門ユーザー・グループ、ラボ・グループ、および開発グループなどです。このような編成を使用することにより、ネットワーク振る舞いを区別したり、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。

大規模なネットワーク・グループでは、各オブジェクトの詳細情報を表示するのが困難になる場合があります。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。

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・グループにまとめて、 ディスク・スペースを節約します。例えば、以下のようにします。

表 *24.* 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

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。

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。例えば、以下のようにします。

表 *25. 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

この例にネットワーク (人事部門の 10.10.50.0/24 など) を追加する場合、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ルールがデフォルトで適用されます。

関連概念:

229 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 **(Define network hierarchy)**」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が、その変更をデプロイするには、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。

許容される **CIDR** 値

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 *26.* 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

表 26. 許容される CIDR 値 (続き)

CIDR の長さ	マスク	ネットワークの数	ホスト数
/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:

『ネットワーク階層の定義』

QRadar では、ネットワーク階層内のすべてのネットワークがローカルとして解釈されます。誤ったオフェンスを防ぐために、ネットワーク階層を常に最新の状態に保持してください。

ネットワーク階層の定義

QRadar では、ネットワーク階層内のすべてのネットワークがローカルとして解釈されます。誤ったオフェンスを防ぐために、ネットワーク階層を常に最新の状態に保持してください。

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。

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. 「ネットワーク階層 **(Network Hierarchy)**」アイコンをクリックします。
4. 「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。
5. 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。
6. 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:

76 ページの『許容される CIDR 値』
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。

QRadar は、システム構成ファイルを使用して、ネットワーク・データ・フローの実用的な特性を設定します。

自動更新の要件

更新を受信するには、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、以下の Web サイトから手動でダウンロードできます。

IBM Fix Central (http://www.ibm.com/support/fixcentral)

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、デプロイメント・エディターを使用してデプロイメントが定義されている場合は、コンソールが管理対象ホストを更新します。デプロイメント・エディターについて詳しくは、 149 ページの『第 11 章 デプロイメント・エディター』を参照してください。

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。

- 構成の更新。構成ファイルの変更、脆弱性、QID マップ、およびセキュリティー脅威情報の更新が含まれます。
- DSM の更新。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。
- メジャー更新。更新された JAR ファイルなどの項目が含まれます。
- マイナー更新。追加のオンライン・ヘルプ・コンテンツや更新されたスクリプトなどの項目が含まれます。

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:

86 ページの『QRadar 更新サーバーのセットアップ』
インターネットにアクセスできない QRadar コンソールがデプロイメント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、QRadar 更新サーバーをセットアップして更新プロセスを管理することができます。

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、 84 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 27. 「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、 85 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、 84 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、 83 ページの『更新のスケジュール』を参照してください。
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、 83 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できます。

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。
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. 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。
11. 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 **(Auto Restart Service)**」チェック・ボックスを選択します。
12. 「拡張」タブをクリックします。
13. 「**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。
14. 「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。
15. 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。 プロキシー・サーバーが必要となるのは、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です。

16. 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。 ユーザー名が必要となるのは、認証済みプロキシーを使用している場合です。
17. 「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。 パスワードが必要となるのは、認証済みプロキシーを使用している場合です。
18. 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。
19. 「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。
20. 「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。
21. 「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。
22. 「保存」をクリックします。

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、Fix Central 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。

QRadar 更新サーバーのセットアップ

インターネットにアクセスできない QRadar コンソールがデプロイメント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、QRadar 更新サーバーをセットアップして更新プロセスを管理することができます。

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。

Fix Central 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:

79 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 サーバーを構成するには、以下のタスクを実行します。更新ディレクトリーを作成し、Fix Central から自動更新パッケージをダウンロードする必要があります。

このタスクについて

自動更新は Fix Central で入手できます。

手順

1. Apache サーバーにアクセスします。 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。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. `autoupdates/` という名前の更新ディレクトリーを作成します。
3. 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。
4. 次の Fix Central から自動更新パッケージをダウンロードします。 http://www.ibm.com/support/fixcentral 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。
5. 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。
6. Apache サーバーで、コマンド **`tar -zxf updatepackage-[timestamp].tgz`** を入力して自動更新パッケージを解凍します。

7. 「管理」タブをクリックします。
8. 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。
9. 「自動更新」をクリックします。
10. 「設定の変更」をクリックします。
11. 「拡張」タブを選択します。
12. 更新プロセスの対象を Apache サーバーにするには、「サーバー構成 **(Server Configuration)**」パネルで、以下のパラメーターを構成します。
    a. 「**Web** サーバー」フィールドで、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 `:<portnumber>` を追加します。
    `https://qmmunity.q1labs.com/:8080`
    b. 「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。
    c. 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。 プロキシー・サーバーが必要となるのは、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です。
    d. 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。 ユーザー名が必要となるのは、認証済みプロキシーを使用している場合です。
    e. オプション: 「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。 パスワードが必要となるのは、認証済みプロキシーを使用している場合です。
13. 「変更のデプロイ」をクリックします。
14. 「保存」をクリックします。
15. SSH を使用して、root ユーザーとして QRadar にログインします。
16. コマンド **`/opt/qradar/bin/UpdateConfs.pl -change_username <username>`** 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。
17. コマンド **`/opt/qradar/bin/UpdateConfs.pl -change_password <password>`** 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。
18. コマンド **`lynx https://<your update server>/<directory path to updates>/manifest_list`** を入力して更新サーバーをテストします。
19. 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 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。
- 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 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. 次の Fix Central から自動更新パッケージをダウンロードします。http://www.ibm.com/support/fixcentral 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. 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。
8. 「自動更新」をクリックします。
9. 「設定の変更」をクリックします。
10. 「拡張」タブを選択します。
11. 「**Web** サーバー」フィールドで、https://localhost/ と入力します。
12. 「フィードの送信 **(Send feed)**」チェック・ボックスをクリアします。

新規更新の追加

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 QRadar をセットアップする必要があります。

手順

1. 次の Fix Central から自動更新パッケージをダウンロードします。http://www.ibm.com/support/fixcentral 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. コマンド **tar -zxf autoupdate-[timestamp].tgz** を入力して自動更新パッケージを解凍します。
4. root ユーザーとして QRadar にログインします。
5. コマンド **lynx https://<your update server>/<directory path to updates>/manifest_list** を入力して更新サーバーをテストします。
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。
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

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。

```
service tomcat restart
```

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。

制約事項**:** 右クリック・メニューにオプションを追加できるのは、QRadar コンソール アプライアンスだけです。また、追加先の対象となるのは、Ariel データベースの一部のフィールドだけです。

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 *28. 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。	
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・メニューに表示す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=$sourceIP$`

表 28. *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
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 のユーザー・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 (QVM 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、UI を使用して手動で削除することができます。

表 29. 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。
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 29. 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。 この値が影響を与える可能性があるアセットのプロパティーを以下に示します。 • 指定された名前 (Given Name) • 統一名 • 重み (Weight) • 説明 • ビジネス・オーナー (Business Owner) • ビジネス担当者 (Business Contact) • テクニカル・オーナー (Technical Owner) • 技術担当者 • ロケーション • 検出信頼性 (Detection Confidence) • ワイヤレス AP (Wireless AP) • ワイヤレス SSID (Wireless SSID) • スイッチ ID (Switch ID) • スイッチ・ポート ID (Switch Port ID) • CVSS 機密性要件 • CVSS 整合性要件 • CVSS 可用性要件 • CVSS 二次的被害の可能性 • テクニカル・ユーザー (Technical User) • ユーザー指定の OS • OS オーバーライド・タイプ (OS Override Type) • OS オーバーライド ID (Override Id) • 拡張 • レガシー (7.2 より前) Cvss リスク (Legacy (Pre-7.2) Risk) • VLAN • アセット・タイプ
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。 アセット製品には、以下のものが含まれます。 • アセットの OS • アセットのインストールされたアプリケーション • アセットの開いているポートに関連付けられている製品

表 29. 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「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 UI 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

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・インターフェースへの root アクセス権限が必要です。

手順

1. root ユーザーとして QRadar にログインします。
2. /etc/ ファイルに、次のコマンドを入力します。

   ```
   vim loginMSG
   ```

   Vim エディターによって、loginMsg ファイルが作成されます。特殊文字を使用したファイル名を指定しないでください。
3. i を押して、メッセージを入力します。
4. メッセージを保存するには、ESC を押します。
5. コマンド・ラインに戻るには、次のコマンドを入力します。

   ```
   :wq
   ```
6. Enter を押します。
7. 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。
8. 「認証設定」をクリックします。
9. 「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
   ```
10. 「保存」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 サーバー証明書の構成

「システム設定」ウィンドウで IF-MAP 認証を構成する前に、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 (例えば、ifmapserver.cert など)。

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. 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

このタスクでは、 IF-MAP 証明書を相互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 (例えば、ifmapserver.cert など)。

相互認証では、コンソールと IF-MAP サーバーに証明書構成が必要です。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。

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/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. 次のコマンドを使用して、Public Key Cryptography Standard ファイル (ファイル拡張子は .pkcs12) を作成します。`openssl pkcs12 -export -inkey <private_key> -in <certificate> -out <pkcs12_filename.pkcs12> -name "IFMAP Client"`
5. 次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. 次のコマンドを入力して、ディレクトリーの権限を変更します。`chmod 755 /opt/qradar/conf/trusted_certificateschmod 644 /opt/qradar/conf/trusted_certificates/*.cert`
8. 次のコマンドを入力して、Tomcat サービスを再始動します。`service tomcat restart`

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 *30. 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。

表 30. QRadar でサポートされる証明書 (続き)

証明書	説明
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:

   ```
   Provide the following information prompted in the command-line:
   [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、-b 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。

  – SSLCertifficateFile
  – 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@csd2-primary ssl]# ls
cert.cert cert.key
[root@qradar ssl]# /opt/qradar/bin/install_ssl_cert.sh -b
Path to private key file (SSLCertificateKeyFile): /root/ssl/cert.key
Path to public key file (SSLCertificateFile): /root/ssl/cert.cert
```

出力例:

```
You have specified the following:
SSLCertificateKeyFile of '/root/ssl/cert.key'
SSLCertificateFile of '/root/ssl/cert.cert'
Continue and reconfigure Apache now (includes restart of httpd daemon)
(Y/[N])? y
Restarting Apache
Stopping httpd: [ OK ]
Starting httpd: [ OK ]
Waiting for Apache to be running . done!
Stopping hostcontext
[Q] Shutting down hostcontext service: Sending SIGQUIT to h[ OK ]xt
[Q] Shutting down hostcontext service: [ OK ]
```

```
Restarting Tomcat
Sending SIGQUIT to tomcat [ OK ]
Stopping httpd: [ OK ]
Shutting down tomcat: [ OK ]
Starting tomcat: [ OK ]
Starting httpd: [ OK ]
Restarting hostcontext
[Q] Starting hostcontext service: [ OK ]
Restarting hostcontext on 172.16.77.105
OK: Successfully applied custom SSL certificate.
[root@qradar ssl]#
```

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』

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

103 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。

アドレスが存在しない場合、無駄なスペースが生じるのを避けるためにテンプレート・ベースのレコードが使用されます。 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、「ログ・ソース・ユーザーズ・ガイド」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。

デプロイメント・エディター

デプロイメント・エディターは、IPv6 アドレスをサポートします。

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. 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. デプロイメント・エディターを使用して、管理対象ホストを追加します。

データ保存

特定のデータのカスタム保存期間を構成します。

保存バケットは、カスタム・フィルター要件と一致するイベントおよびフローの保存ポリシーを定義します。 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・フィルターと一致する場合は、保存ポリシーの期間が満了するまで、その保存バケットに保管されます。この機能により、複数の保存バケットを構成することができます。

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、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。

保存バケットの構成

デフォルトで、「イベント保存」ウィンドウと「フロー保存」ウィンドウには、デフォルトの保存バケットと 10 個の未構成の保存バケットがあります。保存バケットを構成するまで、すべてのイベントまたはフローは、デフォルトの保存バケットに保管されます。

このタスクについて

「イベント保存」ウィンドウと「フロー保存」ウィンドウには、各保存バケットの以下の情報があります。

表 *31.* 保存ウィンドウのパラメーター

パラメーター	説明
順序 (Order)	保存バケットの優先順位。
名前	保存バケットの名前。
保存	保存バケットの保存期間。
圧縮	保存バケットの圧縮ポリシー。
削除ポリシー	保存バケットの削除ポリシー。
フィルター (Filters)	保存バケットに適用されるフィルター。適用されるフィルターについて詳しくは、マウス・ポインターを「フィルター **(Filters)**」パラメーターの上に移動します。
配布	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。
有効	保存バケットが有効 (true) か無効 (false) かを示します。
作成日 (Creation Date)	保存バケットが作成された日時。
変更日 (Modification Date)	保存バケットが最後に変更された日時。

ツールバーには、以下の機能が用意されています。

表 *32.* 保存ウィンドウのツールバー

機能	説明
編集	保存バケットを編集する。
有効/無効	保存バケットを有効または無効にする。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データは、プロパティーと一致する次のバケットに保管されます。
削除	保存バケットを削除する。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」または「フロー保存」アイコンをクリックします。
4. 選択可能な最初の保存バケットをダブルクリックします。
5. 以下のパラメーターを構成します。

パラメーター	説明 *(Description)*
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	保存期間を選択します。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。
このバケット内のデータの圧縮を許可	このチェック・ボックスを選択してデータ圧縮を有効にして、リスト・ボックスから時間フレームを選択します。この時間フレームが経過すると、保存バケット内のすべてのデータが圧縮の対象になります。指定した期間内にデータの圧縮を行わないことによって、システムのパフォーマンスが向上します。圧縮が行われるのは、使用ディスク・スペースがペイロードの場合は 83%、レコードの場合は 85% に達した場合のみです。

パラメーター	説明 *(Description)*
このバケットのデータを削除	削除ポリシーを選択します。 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、「このバケット内のデータの保存期間 *(Keep data placed in this bucket for)*」パラメーターと一致するデータをストレージに残しておく場合は、「ストレージ・スペースが必要な場合」を選択します。使用ディスク・スペースが、レコードの場合は 85%、ペイロードの場合は 83% に達すると、データが削除されます。削除は、ディスク・スペースがレコードの場合は 82%、ペイロードの場合は 81% に達するまで続けられます。 「このバケット内のデータの保存期間 **(Keep data placed in this bucket for)**」パラメーターと一致し次第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、空きディスク・ペースまたは圧縮要件とは関係なく、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。 ストレージが必要な場合は、「このバケット内のデータの保存期間 **(Keep data placed in this bucket for)**」パラメーターと一致するデータのみが削除されます。
説明	保存バケットの説明を入力します。

パラメーター	説明 *(Description)*
現在のフィルター (Current Filters)	フィルターを構成します。 最初のリストで、フィルター対象のパラメーターを選択します。例えば、「デバイス (Device)」、「ソース・ポート (Source Port)」、または「イベント名 (Event Name)」などです。 2 番目のリストで、フィルターに使用する修飾子を選択します。修飾子のリストは、最初のリストで選択した属性によって異なります。 テキスト・フィールドに、フィルターに関連した具体的な情報を入力してから「フィルターの追加 **(Add Filter)**」をクリックします。 フィルターが「現在のフィルター **(Current Filters)**」テキスト・ボックスに表示されます。「現在のフィルター **(Current Filters)**」テキスト・ボックスからフィルターを削除するには、フィルターを選択して「フィルターの削除 **(Remove Filter)**」をクリックします。

6. 「保存」をクリックします。
7. 再度「保存」をクリックします。

   保存バケットが、保存パラメーターと一致するデータの保管を直ちに開始します。

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. アイコンをクリックします。

5. 必要な保存バケットを選択し、正しい場所に移動します。

保存バケットの編集

必要に応じて、保存バケットのパラメーターを編集できます。

このタスクについて

「保存パラメーター (Retention Parameters)」ウィンドウには、デフォルトの保存バケットの編集時に「現在のフィルター (Current Filters)」ペインは表示されません。

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、「データ・ソース」をクリックします。
3. 次のオプションのいずれかを選択してください。
4. 「イベント保存」アイコンをクリックします。
5. 「フロー保存」アイコンをクリックします。
6. 編集する保存バケットを選択して、「編集」をクリックします。
7. パラメーターを編集します。詳しくは、 105 ページの『保存バケットの構成』を参照してください。
8. 「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. 次のオプションのいずれかを選択してください。
4. 「イベント保存」アイコンをクリックします。
5. 「フロー保存」アイコンをクリックします。
6. 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。

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. 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 33. 「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。
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。
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。

表 33. 「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
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「値が次の場合に応答」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。
「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

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**:** 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、行った変更が自動的にステージング・エリアに適用されます。ステージング・エリアから、QRadar デプロイメント・エディターを使用してデプロイ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 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、<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。

   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 property を True に設定します。
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、件名エレメントを編集します。

e. 本文エレメントに対して、パラメーターの追加または削除を行います。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 *34.* 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
Destination		SourcePrecedence
DestinationPort		DestinationTOS
DestinationIP		DestinationDSCP

表 34. 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
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 35. 「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 **(Custom Offense Close Reasons)**」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 **(Custom Offense Close Reasons)**」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 **(Custom Offense Close Reasons)**」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 (Index Management)」機能により、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できます。

イベント・プロパティーとフロー・プロパティーを索引付けすることにより、検索を最適化できます。「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。

「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。
   - 「索引の有効化 **(Enable Index)**」をクリックします。
   - 「索引の無効化 **(Disable Index)**」をクリックします。
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. 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

IBM Security QRadar 製品がペイロード索引を保管する期間を構成することができます。

デフォルトでは、ペイロード索引は 1 週間保存されます。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。

第 7 章 リファレンス・セット管理

「リファレンス・セット管理」ウィンドウを使用して、リファレンス・セットの作成と管理を行うことができます。外部ファイルからリファレンス・セットにエレメントをインポートすることもできます。

リファレンス・セットとは、ネットワーク上で発生したイベントとフローから派生する一連のエレメントのことです。イベントから派生するエレメントの例は、IP アドレスやユーザー名です。

リファレンス・セットを作成すると、そのリファレンス・セットに関連するログ・アクティビティーまたはネットワーク・アクティビティーを検出するためのルールを作成できるようになります。例えば、ネットワーク・リソースにアクセスしようとする無許可のユーザーを検出するためのルールを作成することができます。ログ・アクティビティーまたはネットワーク・アクティビティーがルール条件と一致する場合、エレメントをリファレンス・セットに追加するためのルールを構成することもできます。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。ルールの構成について詳しくは、製品の「ユーザーズ・ガイド」を参照してください。

リファレンス・セットの追加

「管理」タブから、ルールのテストに組み込むことができるリファレンス・セットを追加することができます。

このタスクについて

作成されたリファレンス・セットは、「リファレンス・セット管理」ウィンドウにリストされます。ルールウィザードでは、このリファレンス・セットは「ルールの応答」ページのオプションとしてリストされます。このリファレンス・セットにエレメントを送信するためのルールを 1 つ以上構成すると、「エレメント数」、「関連付けられているルール」、および「容量」の各パラメーターが自動的に更新されます。

手順

1. 「リファレンス・セット管理」ウィンドウで、「追加」をクリックします。
2. 以下のパラメーターを構成します。

表 *36.* 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	このリファレンス・セットの固有名。

表 36. 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	選択できるリファレンス・セット・エレメントのタイプには以下の 5 つがあります。 • 英数字 - 英数字の値の集合 • 数値 - 数値の集合 • **IP** - IP アドレスの集合 • ポート - ポート番号の集合 • 英数字 **(**大/小文字は無視**)** - 英数字の値の集合 (ただしテストでは大/小文字の区別は無視) 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。
エレメントの存続時間	このパラメーターを使用して、**time_to_live** 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かを指定します。 • 最初の表示以降 - エレメントが最初にリファレンス・セットに挿入された時間以降 • 最後の表示以降 - エレメントが最後のリファレンス・セットに挿入された時間以降 リファレンス・セット・エレメントの有効期限が切れると、リファレンス・セット名とエレメント値を含む「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。 デフォルトでは、すべてのエレメントは永久に保存されます。「永久に存続」チェック・ボックスをクリアしないと、エレメントの期限は切れません。

3. 「作成」をクリックします。

エレメントの期限切れイベント

リファレンス・セット内のエレメントの期限が切れたときに作成されるイベントを使用して、ネットワーク内の期限切れユーザー・アカウントを追跡したりすることができます。

デフォルトでは、すべてのリファレンス・セット・エレメントは永久に存続します。つまり、エレメントは削除されるまでリファレンス・セット内に存在します。ただし、エレメントの存続時間を設定して、エレメントの有効期限が切れたときにリファレンス・セット名とエレメント値が含まれたイベントが作成されるようにすることができます。

これらのイベントを使用して、例えば以下のようにしてネットワーク・アカウントが使用されていないことを検出できます。

1. 有効期限が切れたユーザーを追跡するためのリファレンス・セットを作成します。アカウントの適正な非アクティブ期間を表すエレメントの存続時間を設定します。
2. ログイン・データ (**username** など) をリファレンス・セットにエレメントとして追加するカスタム・イベント・ルールを作成します。
3. 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。
4. その後、「ログ・アクティビティー」タブを使用してイベントを追跡できます。

リファレンス・セットの編集

「リファレンス・セット管理」ウィンドウを使用して、リファレンス・セットを編集します。

手順

1. 「リファレンス・セット管理」ウィンドウで、リファレンス・セットを選択します。
2. 「編集」をクリックします。
3. パラメーターを編集します。

表 *37.* 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	このリファレンス・セットの固有名。 255 文字以内で入力してください。
タイプ	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。
エレメントの存続時間 **(Time to Live of Elements)**	リファレンス・セット内で各エレメントを保持する時間。 時間を指定する場合は、エレメントの時間のトラッキングをいつ開始するのかも指定する必要があります。 デフォルトの設定は、「永久に存続」です。

4. 「送信 **(Submit)**」をクリックします。

リファレンス・セットの削除

「リファレンス・セット管理」ウィンドウで、リファレンス・セットを削除することができます。

このタスクについて

リファレンス・セットを削除する場合、削除するリファレンス・セットにルールが関連付けられているかどうかが確認ウィンドウに表示されます。リファレンス・セ

ットを削除すると、「リファレンス・セットに追加 **(Add to Reference Set)**」の構成が、関連付けられているルールから消去されます。

ヒント**:** リファレンス・セットを削除する前に、「参照 **(Reference)**」タブで、関連付けられているルールを確認できます。

手順

次のオプションのいずれかを選択してください。

- 「リファレンス・セット管理」ウィンドウで、リファレンス・セットを選択して「削除」をクリックします。
- 「リファレンス・セット管理」ウィンドウで、「クイック検索 **(Quick Search)**」テキスト・ボックスを使用して削除したいリファレンス・セットだけを表示し、「リスト内容の削除」をクリックします。

リファレンス・セットの内容の表示

「内容」タブには、このリファレンス・セットに含まれているエレメントのリストが表示されます。

手順

1. 「リファレンス・セット管理」ウィンドウで、リファレンス・セットを選択します。
2. 「内容の表示」をクリックします。
3. 内容を表示するには、「内容」タブをクリックします。

   ヒント**:**「クイック検索」フィールドを使用して、特定のエレメントをフィルタリングします。入力したキーワードに一致するすべてのエレメントが「内容」リストに一覧表示されます。その後、ツールバーからアクションを選択できます。

表 *38.* 「内容」タブのパラメーター

パラメーター	説明
値	エレメントの値。 例えば、IP アドレスのリストがリファレンスに含まれている場合、この値は IP アドレスです。
オリジン	ルールへの応答として、「***rulename***」がリファレンス・セットに配置されます。 「ユーザー」が、外部ファイルからインポートされるか、手動でリファレンス・セットに追加されます。
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、リファレンスを表示します。

ヒント: 「クイック検索」フィールドを使用して、特定のエレメントをフィルタリングします。入力したキーワードに一致するすべてのエレメントが「内容」リストに一覧表示されます。その後、ツールバーからアクションを選択できます。

表 *39.* 「内容」タブのパラメーター

パラメーター	説明
ルール名	このルールの名前。
グループ	このルールが属するグループの名前。
カテゴリー	ルールのカテゴリー。オプションには、「カスタム・ルール」と「アノマリ検出ルール」があります。
タイプ	このルールのタイプ。
有効	ルールが有効か無効かを示します。
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ます。

   「ルール」ウィザードで、ルールの構成設定を編集できます。

リファレンス・セットへのエレメントの追加

「リファレンス・セット管理」ウィンドウを使用して、エレメントをリファレンス・セットに追加することができます。

手順

1. 「リファレンス・セット管理」ウィンドウで、リファレンス・セットを選択します。
2. 「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. 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を構成します。

パラメーター	説明
値	複数の値を入力する場合は、それぞれの値の間に分離文字を挿入し、その分離文字を「分離文字」フィールドで指定します。
分離文字	「値」フィールドで指定した分離文字を入力します。

6. 「追加」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・セットからエレメントを削除することができます。

手順

1. 「リファレンス・セット管理」ウィンドウで、リファレンス・セットを選択します。
2. 「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. 次のオプションのいずれかを選択してください。
   - エレメントを選択して、「削除」をクリックします。
   - 「クイック検索 **(Quick Search)**」テキスト・ボックスを使用して削除したいエレメントだけを表示し、「リスト内容の削除」をクリックします。
5. 「削除」をクリックします。

リファレンス・セットへのエレメントのインポート

外部の CSV ファイルまたはテキスト・ファイルから、エレメントをインポートすることができます。

始める前に

インポートする CSV ファイルまたはテキスト・ファイルが、ローカルのデスクトップに保管されるようにしてください。

手順

1. 「リファレンス・セット管理」ウィンドウで、リファレンス・セットを選択します。
2. 「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. ツールバーで、「インポート」をクリックします。
5. 「参照 **(Browse)**」をクリックします。
6. インポートする CSV ファイルまたはテキスト・ファイルを選択します。
7. 「インポート」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エクスポート

リファレンス・セットのエレメントは、外部の CSV ファイルとテキスト・ファイルにエクスポートすることができます。

手順

1. 「リファレンス・セット管理」ウィンドウで、リファレンス・セットを選択します。
2. 「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. ツールバーで、「エクスポート」をクリックします。
5. 次のオプションのいずれかを選択してください。
6. リストを開いてすぐに表示したい場合は、「アプリケーションから開く **(Open with)**」オプションを選択して、リスト・ボックスからアプリケーションを選択します。
7. リストを保存する場合は、「ファイルの保存 **(Save File)**」オプションを選択します。
8. 「**OK**」をクリックします。

第 8 章 リファレンス・データ・ユーティリティーによるリファレンス・データ収集の管理

ReferenceDataUtil.sh ユーティリティーを使用して、複雑なリファレンス・データ収集を作成します。

リファレンス・データ・ユーティリティーを使用して、コマンド・ラインからリファレンス・データ収集を管理します。ReferenceDataUtil.sh を使用して、以下のタイプのリファレンス・データ収集を作成できます。

- リファレンス・マップ
- セットのリファレンス・マップ
- マップのリファレンス・マップ
- リファレンス・テーブル

リファレンス・データ収集の作成

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. /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 [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

```
Create an Alphanumeric Map
 ./ReferenceDataUtil.sh create testALN MAP ALN

Create a Map of Sets of PORT values that will age out 3 hours after they
were last seen
 ./ReferenceDataUtil.sh create testPORT MAPOFSETS PORT -timeoutType=LAST_SEEN
-timeToLive='3 hours'

Create a Map of Maps of Numeric values that will age out 3 hours 15 minutes
after they were first seen
 ./ReferenceDataUtil.sh create testNUM MAPOFMAPS NUM -timeoutType=FIRST_SEEN
-timeToLive='3 hours 15 minutes'

Create a ReferenceTable with a default of Alphanumeric values
 ./ReferenceDataUtil.sh create testTable REFTABLE ALN
-keyType=ipKey:IP,portKey:PORT,numKey:NUM,dateKey:DATE
```

次のタスク

ユーザー・インターフェースにログインし、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。ルールおよびルール・テストの作成について詳しくは、製品の「ユーザーズ・ガイド」を参照してください。

ReferenceDataUtil.sh コマンド・リファレンス

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。

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。

[MAP | MAPOFSETS | MAPOFMAPS | REFTABLE]
リファレンス・データ収集のタイプ。

[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、英数字の値のリファレンス・データ収集を指定します。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、英数字の値のリファレンス・データ収集を指定します。ただし、テストでは、大/小文字の区別は無視されます。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、数値のリファレンス・データ収集を指定します。
- **IP** は、IP アドレスのリファレンス・データ収集を指定します。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・アドレスのリファレンス・データ収集を指定します。
- **DATE** は、日付値のリファレンス・データ収集を指定します。

[-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。MAP と MAPOFSETS には、key1 が必要です。MAPOFMAPS と REFTABLE には、key1 と key2 が必要です。各キーは、英数字ストリングです。key2 は第 2 レベルのキーです。MAPOFMAPS または REFTABLE コレクションに対して追加または削除を行うときに、このキーが必要です。

[-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。

delete

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。MAP と MAPOFSETS には、キー 1 が必要です。MAPOFMAPS と REFTABLE には、キー 1 とキー 2 が必要です。各キーは、英数字ストリングです。

[-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。

第 9 章 許可サービスの管理

QRadar デプロイメント向けにお客様サポート・サービスまたは 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。

お客様サポート・サービスを認証すると、サービスの QRadar ユーザー・インターフェースへの接続が可能になり、Web サービスを使用してオフェンスの注釈を取り消しまたは更新することができます。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。

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。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 *40.* 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。

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、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 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、IBM Security 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 10 章 バックアップおよびリカバリーの管理

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。

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・データおよびフロー・データをバックアップできます。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。イベント・データおよびフロー・データのリストアで支援が必要な場合は、データのリストアに関するテクニカル・ノート 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。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。

使用できる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。

構成バックアップには以下のコンポーネントが含まれます。

- 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 (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

バックアップ・アーカイブの管理

バックアップ・アーカイブの表示と管理

「アーカイブのバックアップ」ウィンドウから、成功したすべてのバックアップ・アーカイブを表示および管理することができます。

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 **(Backup and Recovery)**」アイコンをクリックします。

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 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 **(Backup and Recovery)**」アイコンをクリックします。
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。

バックアップ・アーカイブの作成

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。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。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 41. 「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	

表 41. 「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・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、「*Offboard Storage Guide*」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。
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。

表 41. 「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
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。
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

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 **(Backup and Recovery)**」アイコンをクリックします。
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。 136 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・アーカイブのリストア

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 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、IBM Security 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 IBM Security 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。イベント・データまたはフロー・データのリストアについては、データのリストアに関するテクニカル・ノート 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。

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 42. 「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。
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 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 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 *43.* 「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 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。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。
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。
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

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 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ため、ls -l と入力します。
4. バックアップ・ファイルがリストされたら、cd / と入力してルート・ディレクトリーに移動します。

   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 45. 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
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。

表 45. ファイル名の変数についての説明 (続き)

ファイル名の変数	説明
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。

第 11 章 デプロイメント・エディター

デプロイメント・エディターを使用して、QRadar の個々のコンポーネントを管理します。デプロイメントを構成した後、デプロイメントで各管理対象ホスト内の個々のコンポーネントにアクセスして、構成できます。

デプロイメント・エディターの要件

デプロイメント・エディターを使用する前に、デプロイメント・エディターが最小システム要件を満たしていることを確認してください。

デプロイメント・エディターには、Java™ ランタイム環境 (JRE) が必要です。Java Web サイト (www.java.com) から、Java 1.6 または 1.7 をダウンロードできます。 Mozilla Firefox Web ブラウザーを使用している場合は、Java Network Language Protocol (JNLP) ファイルを受け入れるようにブラウザーを構成する必要があります。

Microsoft Internet Explorer エンジンを使用する Maxthon などの多くの Web ブラウザーでは、「管理」タブと互換性を持たない可能性のあるコンポーネントがインストールされます。システムにインストールされた Web ブラウザーを無効にする必要が生じることがあります。

プロキシー・サーバーまたはファイアウォールの背後からデプロイメント・エディターにアクセスするには、デスクトップに適切なプロキシー設定を構成する必要があります。これにより、ソフトウェアはプロキシー設定をブラウザーから自動的に検出できます。

プロキシー設定を構成するには、「コントロール パネル」にある Java 構成を開き、プロキシー・サーバーの IP アドレスを構成します。詳しくは、Microsoft の資料を参照してください。

デプロイメント・エディターのビュー

デプロイメント・エディターは、デプロイメントの各種ビューを提供します。

「管理」タブを使用して、デプロイメント・エディターにアクセスできます。デプロイメント・エディターを使用してデプロイメントを作成し、接続を割り当て、各コンポーネントを構成します。

デプロイメント・エディターを使用して構成設定を更新した後、それらの変更をステージング・エリアに保存する必要があります。「管理」タブのメニュー・オプションを使用して、すべての変更を手動でデプロイする必要があります。デプロイされると、すべての変更がデプロイメント全体で有効になります。

デプロイメント・エディターは以下のビューを提供します。

システム・ビュー (System View)

「システム・ビュー (System View)」ページを使用して、デプロイメント内の管理対象ホストにソフトウェア・コンポーネントを割り当てます。「システム・ビュー (System View)」ページには、デプロイメント内のすべての管理対象ホストが含まれています。管理対象ホストは、QRadar ソフトウェアがインストールされているデプロイメント内のシステムです。

デフォルトで、「システム・ビュー (System View)」ページには以下のコンポーネントも含まれています。

- ホスト・コンテキスト **(Host Context)** - すべての QRadar コンポーネントをモニターし、各コンポーネントが期待通りに機能していることを確認します。
- アキュムレーター - フロー、イベント、レポート作成、データベース・データの書き込み、およびデバイス・サポート・モジュール (DSM) のアラートを分析します。

  アキュムレーターは、イベント・プロセッサー・プログラムが含まれるすべてのホスト上に配置されています。

「システム・ビュー (System View)」ページの左ペインには、表示および構成できる管理対象ホストのリストがあります。デプロイメント・エディターは、管理対象ホストに対する更新がないかデプロイメントをポーリングします。デプロイメント・エディターによってデプロイメント内の管理対象ホストに対する変更が検出されると、その変更を通知するメッセージが表示されます。例えば、管理対象ホストを削除すると、そのホストに割り当てられたコンポーネントを別のホストに再割り当てする必要があることを示すメッセージが表示されます。

また、管理対象ホストをデプロイメントに追加すると、管理対象ホストが追加されたことを示すメッセージがデプロイメント・エディターによって表示されます。

イベント・ビュー (Event View)

「イベント・ビュー (Event View)」ページを使用して、コンポーネントのビューを作成します。

- QRadar QFlow Collector コンポーネント
- イベント・プロセッサー
- QRadar Event Collector
- オフサイト・ソース
- オフサイト・ターゲット
- 判定機能 コンポーネント
- データ・ノード

「イベント・ビュー (Event View)」ページの左ペインには、ビューに追加できるコンポーネントのリストがあります。右ペインには、デプロイメントのビューが示されます。

脆弱性ビュー (Vulnerability View)

「脆弱性ビュー (Vulnerability View)」ページを使用して、IBM Security QRadar Vulnerability Manager コンポーネントのビューを作成します。このビューを表示するには、IBM Security QRadar Vulnerability Manager をインストールする必要があります。詳しくは、「*IBM Security QRadar Vulnerability Manager User Guide*」を参照してください。

デプロイメント・エディターの設定の構成

デプロイメント・エディターの設定を構成して、ズーム増加とプレゼンスのポーリング頻度を変更できます。

手順

1. 「ファイル」 > 「設定の編集 **(Edit Preferences)**」を選択します。
2. 「プレゼンスのポーリング頻度 **(Presence Poll Frequency)**」パラメーターを構成するには、管理対象ホストがデプロイメント環境内の更新をモニターする頻度をミリ秒単位で入力します。
3. 「ズーム増加 **(Zoom Increment)**」パラメーターを構成するには、ズーム・オプションを選択した場合に増加値を入力します。

   例えば、0.1 は 10% を示します。

デプロイメント・エディターを使用したデプロイメントの作成

「管理」タブの「デプロイメント・エディター」を使用して、IBM Security QRadar デプロイメント環境内のコンポーネントを追加および構成します。また、「デプロイメント・エディター」を使用してデプロイメントの可視化を行うこともできます。

始める前に

既存のデプロイメントに管理対象ホストを追加するか、デプロイメントに QRadar Event Collector、フロー・プロセッサー、またはその他のアプライアンスを追加するには、「管理」タブの「システムおよびライセンス管理」ツールで「デプロイメント・アクション」を使用します。

デプロイメント・エディターを使用する前に、以下の条件を満たしていることを確認してください。

- Java ランタイム環境 (JRE) をインストールします。Java Web サイト (www.java.com) から、Java 1.6 または 1.7 をダウンロードできます。
- Firefox ブラウザーを使用している場合は、Java Network Language Protocol (JNLP) ファイルを受け入れるようにブラウザーを構成する必要があります。
- QRadar のデプロイメントについての計画を立てます。これには、デプロイメント内のすべてのデバイスの IP アドレスやログイン情報が含まれます。

手順

1. 「管理」タブをクリックし、「デプロイメント・エディター」をクリックします。

2. 「イベント・ビュー **(Event View)**」タブをクリックし、イベント・コンポーネントをデプロイメントに追加します。
3. 「システム・ビュー **(System View)**」タブをクリックし、システムをビルドします。
4. コンポーネントを構成します。
5. デプロイメントをステージングするには、「デプロイメント・エディター」で「ファイル」 > 「ステージングに保存 **(Save to Staging)**」をクリックします。
6. QRadar コンソール の「管理」タブで以下のオプションのいずれかを選択して構成をデプロイします。
   - 「変更のデプロイ」をクリックする。
   - 「拡張」 > 「すべての構成のデプロイ」をクリックする。

   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:

58 ページの『インストール後の管理対象ホストおよびコンポーネントのデプロイ』

インストール後に、管理対象ホストをデプロイメント環境に追加することができます。分散処理を支援するため、QRadar Event Collector、QRadar フロー・プロセッサー、または他のアプライアンスをデプロイメント環境に追加することができます。

QRadar 製品の公開鍵の生成

IBM Security QRadar のデプロイメント・エディター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。

イベント・ビューの管理

「イベント・ビュー (Event View)」ページを使用して、デプロイメント用のコンポーネントを作成および管理します。

イベント・ビューの作成

「イベント・ビュー (Event View)」を作成するには、以下の手順を実行します。

1. コンポーネントをビューに追加します。
2. コンポーネントを接続します。
3. デプロイメントを接続します。
4. 各コンポーネントの名前が一意になるように、コンポーネントの名前を変更します。

デプロイメント内の QRadar コンポーネントのイベント・ビュー

「イベント・ビュー (Event View)」ページを使用して、QRadar QFlow Collector、イベント・プロセッサー、QRadar Event Collector、オフサイト・ソース、オフサイト・ターゲット、および 判定機能コンポーネントを含む IBM Security QRadar コンポーネントのビューを作成します。

QRadar QFlow Collector

QRadar VFlow 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。

QRadar QFlow Collector は、関連する個々のパケットをグループ化して 1 つのフローにまとめます。QRadar QFlow Collector が、固有ソース IP アドレス、宛先 IP アドレス、ソース・ポート、宛先ポート、および他の特定のプロトコル・オプションを持つ最初のパケットを検出すると、フローが開始します。

新しい各パケットが評価されます。バイト数とパケット数がフロー・レコードの統計カウンターに追加されます。統計間隔の最後に、フローの状況レコードがイベント・コレクターに送信され、フローの統計カウンターがリセットされます。構成された時間内にフローのアクティビティーが検出されなくなると、フローが終了します。

使用するプロトコルでポート・ベースの接続がサポートされていない場合、QRadar は 2 つのホスト間のすべてのパケットを結合して 1 つのフロー・レコードにします。ただし、QRadar QFlow Collector は、別の QRadar コンポーネントへの接続が確立されてデータが取得されるまで、フローを記録しません。

イベント・コレクター

ログ・ソースと呼ばれる、ネットワーク上のセキュリティー・デバイスからセキュリティー・イベントを収集します。

イベント・コレクターは収集されたイベントを正規化し、イベント・プロセッサー・プログラムに情報を送信します。

非コンソール・イベント・プロセッサー・プログラムを、QRadar コンソール上のイベント・プロセッサー・プログラム、またはデプロイメント内の別のイベント・プロセッサー・プログラムに接続することができます。イベント・プロセッサー・プログラムからのフローとイベント情報の収集は、アキュムレーターが行います。

QRadar コンソールのイベント・プロセッサー・プログラムは常に判定機能に接続されています。この接続を削除することはできません。

データ・ノード

データ・ノードは、関連するイベント・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ます。

データ・ノードは、このセキュリティー・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・プログラム・コンポーネントまたはフロー・プロセッサー・コンポーネントに接続されています。

オフサイト・ソース

正規化されたデータをイベント・コレクターに転送するオフサイトのデータ・ソース。データを受け取った後暗号化してからデータを転送するように、オフサイト・ソースを構成することができます。

新しいバージョンの QRadar システムは、それより前のバージョンの QRadar システムからのデータを受信することができます。ただし、前のバージョンがそれより新しいバージョンからのデータを受信することはできません。これを避けるために、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。

オフサイト・ターゲット

イベントまたはフロー・データを受信するオフサイト・デバイスを示します。オフサイト・ターゲットは、イベント・コレクターからのデータのみを受信できます。

新しいバージョンの QRadar システムは、それより前のバージョンの QRadar システムからのデータを受信することができます。ただし、前のバージョンがそれより新しいバージョンからのデータを受信することはできません。これを避けるために、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。

判定機能

デプロイメントごとに 1 つの判定機能コンポーネントを追加できます。判定機能には、ネットワーク・トラフィックとセキュリティー・イベントの表示、レポート、アラート、および分析機能が含まれています。判定機能は、応答を作成するように構成されたカスタム・ルールを使用して、イベントまたはフローを処理します。カスタム・ルールがない場合、判定機能はデフォルトのルールセットを使用して、違反しているイベントまたはフローを処理します。

判定機能では応答に優先順位が付けられ、応答の数、重大度、関連性、および信頼性など、いくつかの要因に基づいてマグニチュードの値が割り当てられます。

判定機能によってマグニチュードが設定されると、解決策として複数のオプションが提供されます。

コンポーネントの追加

デプロイメントを構成するときに、デプロイメント・エディターの「イベント・ビュー (Event View)」ページを使用して、コンポーネントを追加する必要があります。

「イベント・ビュー (Event View)」ページに以下の QRadar コンポーネントを追加できます。

- イベント・コレクター
- イベント・プロセッサー・プログラム
- オフサイト・ソース
- オフサイト・ターゲット
- QRadar QFlow Collector
- データ・ノード

手順

1. 「管理」タブで、「デプロイメント・エディター」をクリックします。
2. 「イベント・コンポーネント (Event Components)」ペインで、デプロイメントに追加するコンポーネントを選択します。
3. 追加するコンポーネントに固有の名前を入力して、「次へ」をクリックします。

   制約事項: 名前には最大 20 文字を使用でき、下線またはハイフンを含めることができます。
4. 「割り当てるホストの選択 **(Select a host to assign to)**」リスト・ボックスで管理対象ホストを選択して「次へ」をクリックします。
5. 「終了」をクリックします。
6. ビューに追加する各コンポーネントに対して、ステップ 3 から 5 を繰り返します。
7. デプロイメント・エディターのメニューから、「ファイル」 > 「ステージングに保存 **(Save to Staging)**」を選択します。

   デプロイメント・エディターによってステージング・エリアに変更内容が保存され、エディターが自動的に閉じます。
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。

コンポーネントの接続

必要なすべてのコンポーネントを「イベント・ビュー (Event View)」ページに追加した後、それらを接続する必要があります。

このタスクについて

「イベント・ビュー (Event View)」ページを使用して、複数のコンポーネントを接続します。いくつかの制約事項が適用されます。例えば、イベント・コレクターはイベント・プロセッサー・プログラムには接続できますが、判定機能コンポーネントには接続できません。

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 *46.* サポートされるコンポーネント接続の説明

ソース接続	ターゲット接続	説明
QRadar QFlow Collector	イベント・コレクター	QRadar QFlow Collector が接続できるのは、イベント・コレクターのみです。 QRadar QFlow Collector は、15xx アプライアンスのイベント・コレクターには接続できません。 接続数は制限されません。
イベント・コレクター	イベント・プロセッサー・プログラム	1 つのイベント・コレクターが接続できるイベント・プロセッサー・プログラムは、1 つのみです。 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・プログラムのみに接続できます。この接続を削除することはできません。 非コンソール・イベント・コレクターは、同じシステム上のイベント・プロセッサー・プログラムに接続できます。 イベント・プロセッサー・プログラムがコンソールにまだ存在していない場合にのみ、非コンソール・イベント・コレクターをリモートのイベント・プロセッサー・プログラムに接続できます。
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。

表 46. サポートされるコンポーネント接続の説明 (続き)

ソース接続	ターゲット接続	説明
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 **(Receive Flows)**」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、システムで「イベントの受信 **(Receive Events)**」機能が有効になっている場合、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。
イベント・プロセッサー・プログラム	判定機能 (MPC)	1 つのイベント・プロセッサー・プログラムのみが判定機能に接続できます。
イベント・プロセッサー・プログラム	イベント・プロセッサー・プログラム	コンソール・イベント・プロセッサー・プログラムは、非コンソール・イベント・プロセッサー・プログラムに接続できません。 非コンソール・イベント・プロセッサー・プログラムは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・プログラムに接続できますが、同時に両方に接続することはできません。 非コンソール・イベント・プロセッサー・プログラムは、非コンソール管理対象ホストが追加されるとコンソール・イベント・プロセッサー・プログラムに接続されます。
データ・ノード	イベント・プロセッサー・プログラム	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・ノードを同じイベント・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。

手順

1. 「イベント・ビュー (Event View)」ページで、接続を確立するコンポーネントを選択します。
2. 「アクション」 > 「接続の追加 **(Add Connection)**」をクリックします。

   マップ内に矢印が表示されます。この矢印は、2 つのコンポーネント間の接続を表します。

3. 接続を確立するコンポーネントまで、矢印の端をドラッグします。
4. オプション: QRadar QFlow Collector とイベント・コレクターの間の接続に対して、フロー・フィルター処理を構成します。
   a. QRadar QFlow Collector とイベント・コレクターの間の矢印を右クリックして、「構成」をクリックします。
   b. 「フロー・フィルター **(Flow Filter)**」パラメーターのフィールドに、QRadar QFlow Collector によるフローの送信先となるQRadar Event Collectorの IP アドレスまたは CIDR アドレスを入力します。
5. 「保存」をクリックします。
6. これらのステップを、接続が必要な残りのすべてのコンポーネントに対して繰り返します。

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、受信するデプロイメントで、関連付けられたオフサイト・イベント・コレクターからイベントとフローを受信するよう、現在のデプロイメントでオフサイト・イベント・コレクターを構成します。

このタスクについて

「イベント・ビュー (Event View)」ページに以下のコンポーネントを追加できます。

- オフサイト・ソースは、イベントおよびフロー・データの受信元であるオフサイト・イベント・コレクターです。

  制約事項**:** オフサイト・ソースは、イベントまたはフロー・データをオフサイト・ターゲットに送信するための適切な権限を使用して構成する必要があります。
- オフサイト・ターゲットは、イベントおよびフロー・データの送信先となるオフサイト・イベント・コレクターです。

例**:**

2 つのデプロイメント (A および B) 間で正規化されたイベントおよびフローを転送する場合に、デプロイメント B がデプロイメント A からイベントおよびフローを受信するようにするには、以下の手順を実行します。

1. オフサイト・ターゲットを使用してデプロイメント A を構成し、イベント・コレクター B を含む管理対象ホストの IP アドレスを指定します。
2. イベント・コレクター A をオフサイト・ターゲットに接続します。
3. デプロイメント B で、イベント・コレクター A を含む管理対象ホストの IP アドレスと、イベント・コレクター A がモニターしているポートを使用してオフサイト・ソースを構成します。

オフサイト・ソースを切断する場合、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。デプロイメント A からオフサイト・ターゲットを削除し、デプロイメント B でオフサイト・ソースを削除します。

デプロイメント間の暗号化を有効にするには、オフサイトのソースと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。また、オフサイト・ソース (クライア

ント) の SSH 公開鍵をターゲット (サーバー) に使用して、適切なアクセスを確保できるようにする必要があります。例えば、オフサイト・ソースと イベント・コレクター B の間で暗号化を有効にするには、以下の手順を実行します。

1. **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。これにより、デフォルトでファイルが //root/.ssh ディレクトリーに配置されます。
2. id_rsa.pub ファイルを、イベント・コレクターおよびソース・コンソールの /root/.ssh ディレクトリーにコピーします。ファイル名を authorized_keys に変更します。

   このファイルと親ディレクトリーに rw オーナー特権 (chmod 600 authorized_keys) を割り当てていない場合は、**ssh-copy-id** コマンドを使用することができます。例えば、**ssh-copy-id -i hostUsername@hostIP** などです。**-i** は、アイデンティティー・ファイル /root/.ssh/id_rsa.pub を使用することを指定します。例えば、ssh-copy-id -i root@10.100.133.80 などです。このコマンドにより、すべてのエントリーが追加されるか、またはターゲット・コンソールに適切な特権で authorized_keys ファイルが作成されます。重複エントリーのチェックは行われません。authorized_keys は、他の機能が使用されるコンソール上にも存在している必要があります。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は、そのコンソールの /root/.ssh ディレクトリーにも authorized_keys ファイルが存在している必要があります。このファイルが存在しないと、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間で暗号化を使用するかどうかにかかわらず、このファイルは必要です。
3. ソース・コンソール上で、/opt/qradar/conf ディレクトリーの下に ssh_keys_created ファイルを作成します。他の機能 (コンソールの 1 つに管理対象ホストを追加する機能など) を組み合わせて使用する場合に、イベントおよびフローの転送が中断されないように、このファイルを作成する必要があります。必要な場合は、オーナーとグループを「**nobody**」に変更し、権限を「**775**」に変更します。ファイルのバックアップとリストアを適切に実行できるようにするには、chown nobody:nobody /opt/qradar/conf/ssh_keys_created および chmod 775 /opt/qradar/conf/ssh_keys_created と指定します。
4. 2 つのコンソールについて、オフサイト・ソースとオフサイト・ターゲットの手順を実行します。最初にターゲット・コンソールをプログラムし、その後変更をデプロイします。次にソース・コンソールをプログラムし、その後変更をデプロイします。

以下のダイアグラムは、デプロイメント間でのイベントやフローの転送を示します。

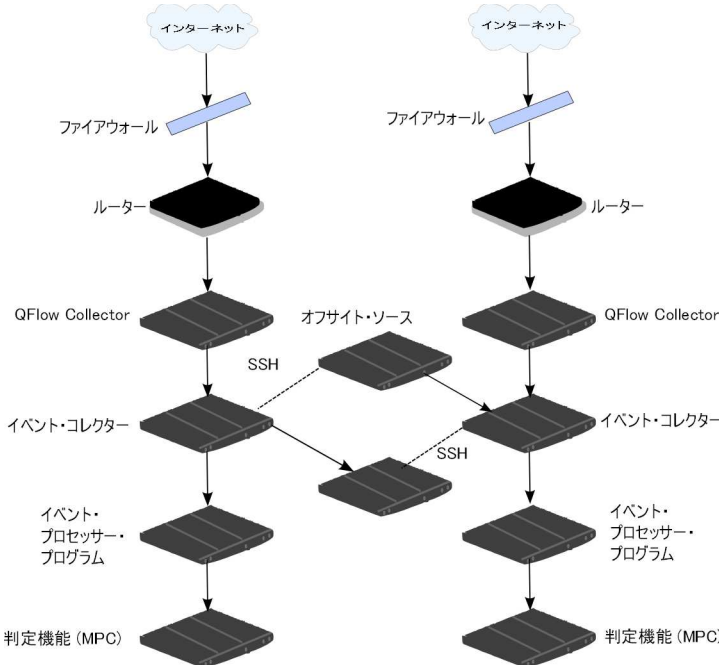

図 *1. SSH* を使用したデプロイメント間のイベントの転送

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。公開鍵の生成について詳しくは、Linux の資料を参照してください。

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、ソースと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。

手順

1. 「管理」タブで、「デプロイメント・エディター」をクリックします。
2. 「イベント・コンポーネント (Event Components)」ペインで、「オフサイト・ソース」または「オフサイト・ターゲット」を選択します。
3. オフサイト・ソースまたはオフサイト・ターゲットの固有の名前を入力します。名前には最大 20 文字を使用でき、下線またはハイフンを含めることができます。「次へ」をクリックします。
4. パラメーターの値を入力して、「終了」をクリックします。

   「オフサイト・ホストの名前を入力 **(Enter a name for the off-site host)**」フィールドのホスト名は最大長 20 文字であり、またアンダースコアーやハイフンの文字を含めることができます。

   「オフサイト・ソースからのトラフィックを暗号化 **(Encrypt traffic from off-site source)**」チェック・ボックスを選択した場合は、関連するオフサイト・ソースとターゲットでも暗号化チェック・ボックスを選択する必要があります。
5. 残りのすべてのオフサイト・ソースとターゲットについて操作を繰り返します。

6. デプロイメント・エディターのメニューから、「ファイル」 > 「ステージングに保存 **(Save to Staging)**」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。

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 情報に基づきます。

「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。

コンポーネントの名前変更

デプロイメント全体でコンポーネントを一意に識別できるように、ビューでコンポーネントの名前を変更する必要があります。

手順

1. 「イベント・コンポーネント (Event Components)」ペインで、名前を変更するコンポーネントを選択します。
2. 「アクション」 > 「コンポーネントの名前変更 **(Rename component)**」をクリックします。
3. コンポーネントの新しい名前を入力します。

   名前は特殊文字を含まない英数字である必要があります。
4. 「**OK**」をクリックします。

データ・リバランスの進行状況の表示

デプロイメント環境にデータ・ノードをインストールしたら、イベント・プロセッサーとデータ・ノード間のデータ移動の進行状況を表示します。データのリバランスが完了すると、デプロイされたデータ・ノードに関する追加情報を表示できるようになります。

手順

1. QRadar コンソールで、「管理」タブをクリックして、ウィンドウの最上部に表示されるデプロイメント内のデータ・ノードの状況を確認します。
2. 「詳細」列の「表示」をクリックして、「システムおよびライセンスの詳細」ウィンドウを開きます。
3. 「セキュリティー・データの配布」ペインで、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確認します。

データ・ノード・コンテンツのアーカイブ

データ・ノード・アプライアンスを「アーカイブ」ノードに設定した場合、アプライアンスにデータは書き込まれません。既存のデータは保存されます。

手順

1. デプロイメント・エディターで、アーカイブ・モードに設定したいデータ・ノードを右クリックし、「構成」をクリックします。
2. 「アーカイブ」をクリックします。
3. 「管理」タブ・メニューで、「変更のデプロイ」をクリックします。
4. アーカイブ・モードになっているデータ・ノードへのデータ分散を再開したい場合は、「構成」 > 「アクティブ」を右クリックします。

イベント・プロセッサー・データをデータ・ノード・アプライアンスに保存する

イベント・プロセッサーではなく、データ・ノード・アプライアンスにすべてのデータを保存することにより、イベント・プロセッサーのパフォーマンスを改善することができます。イベント・プロセッサーと同じクラスター内に使用可能でアクティブなデータ・ノード・アプライアンスが存在しない場合、イベント・プロセッサーはデータをローカルの場所に保存します。いずれかのデータ・ノード・アプライアンスが使用可能な状態になると、そのアプライアンスは可能な限り多くのデータをイベント・プロセッサーから転送します。クラスター内のすべてのデータ・ノードの空き領域が均一になるように、データ・ノード間でデータが分散されます。

手順

1. デプロイメント・エディターで、データ・ノード・アプライアンスに転送したいデータを持つイベント・プロセッサーを右クリックし、「構成」をクリックします。
2. 「アクティブ」をクリックし、リストから「処理のみ **(Processing-Only)**」を選択します。
3. 「管理」タブ・メニューで、「変更のデプロイ」をクリックします。

システム・ビューの管理

システム・ビューのページを使用して、デプロイメント環境内の各管理対象ホスト上で実行するコンポーネントを選択します。

「システム・ビュー (System View)」ページの概要

「システム・ビュー (System View)」ページを使用して、ネットワーク内のすべての管理対象ホストを管理します。

管理対象ホストは、QRadar ソフトウェアを含むネットワーク内のコンポーネントです。QRadar アプライアンスを使用している場合、そのアプライアンス・モデルのコンポーネントが「システム・ビュー (System View)」ページに表示されます。QRadar ソフトウェアがユーザーのハードウェアにインストールされている場合、「システム・ビュー (System View)」ページにはホスト・コンテキスト・コンポーネントが含まれます。

「システム・ビュー (System View)」ページを使用して、以下のタスクを実行します。

- 管理対象ホストをデプロイメントに追加する。
- デプロイメント内で NAT ネットワークを使用する。
- 管理対象ホストのポート構成を更新する。
- コンポーネントを管理対象ホストに割り当てる。
- ホスト・コンテキストを構成する。
- アキュムレーターを構成する。

コンソール・ホストと非コンソール・ホストに対するソフトウェア互換性要件

QRadar のバージョンがコンソール上のバージョンと対応していない場合、非コンソールの管理対象ホスト上でコンポーネントの追加、割り当て、構成を行うことはできません。管理対象ホストに以前はコンポーネントが割り当てられていて、現在は互換性のないバージョンのソフトウェアを実行している場合でも、それらのコンポーネントを表示することができます。ただし、それらのコンポーネントの更新や削除を行うことはできません。

暗号化

暗号化を行うと、管理対象ホスト間のすべてのトラフィックに対するセキュリティーを高めることができます。セキュリティーを強化するために、QRadar は OpenSSH に対応した統合サポートも提供しています。QRadar と統合されることで、OpenSSH はコンポーネント間に保護された通信を提供します。

暗号化はデプロイメント内の管理対象ホスト間で行われるため、暗号化を行うには、デプロイメントが複数の管理対象ホストで構成されている必要があります。暗号化は、クライアントから開始された SSH トンネル (ポート転送) を使用して有効になります。クライアントは、クライアント/サーバーの関係で接続を開始するシステムです。管理対象ホストに対して暗号化が有効な場合、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暗号化トンネルが作成されます。暗号化トンネルは、各サーバーに対する保護されたアクセスを提供します。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。

管理対象ホストで暗号化を有効にすると、クライアント・ホストで暗号化 SSH トンネルが作成されます。例えば、イベント・プロセッサー・プログラムとイベント・コレクターの間の接続、およびイベント・プロセッサー・プログラムと判定機能の間の接続が暗号化されます。QRadar コンソールで暗号化を有効にすると、「オフェンス」タブを使用してイベントを検索する際、暗号化トンネルが使用されます。

ヒント: コンポーネントを右クリックして、コンポーネント間の暗号化を有効にできます。

重要: 暗号化を有効にすると、管理対象ホストのパフォーマンスが少なくとも 50% 低下します。

管理対象ホストの追加

デプロイメント・エディターの「システム・ビュー (System View)」ページを使用して、管理対象ホストを追加します。

始める前に

管理対象ホストに QRadar がインストールされてい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、171 ページの『NAT されたネットワーク』を参照してください。

NAT をサポートしないように構成されているコンソールに NAT された管理対象ホストを追加する場合、そのコンソールで NAT を無効にする必要があります。詳しくは、 173 ページの『管理対象ホストの NAT 状況の変更』を参照してください。

手順

1. 「アクション」 > 「管理対象ホストの追加 **(Add a Managed Host)**」をクリックします。
2. 「次へ」をクリックします。
3. パラメーターの値を入力します。

   以下の表を参照して、パラメーターを構成してください。

表 *47.* 管理対象ホストのパラメーター

パラメーター	説明
ホストを **NAT** する **(Host is NATed)**	この管理対象ホストで既存のネットワーク・アドレス変換 (NAT) を使用する場合に、このチェック・ボックスを選択します。
暗号化を有効にする **(Enable Encryption)**	ホストの SSH 暗号化トンネルを作成する場合に、このチェック・ボックスを選択します。
	2 つの管理対象ホスト間でデータ圧縮を有効にする場合に、このチェック・ボックスを選択します。

4. 「ホストを **NAT** する **(Host is NATed)**」チェック・ボックスを選択した場合は、パラメーターを構成します。

表 *48. NAT* されたネットワークのパラメーター

パラメーター	説明
追加するサーバーまたはアプライアンスのパブリック **IP** を入力 **(Enter public IP of the server or appliance to add)**	管理対象ホストはこの IP アドレスを使用して、NAT を使用するさまざまなネットワークで他の管理対象ホストと通信します。
NAT されたネットワークの選択 **(Select NATed network)**	管理対象ホストがコンソールと同じサブネットにある場合、NAT されたネットワークのコンソールを選択します。 管理対象ホストがコンソールと同じサブネットにない場合、NAT されたネットワークの管理対象ホストを選択します。

5. 「次へ」をクリックします。
6. 「終了」をクリックします。
7. 変更を内容デプロイします。

関連概念:

171 ページの『NAT されたネットワーク』
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。

管理対象ホストの編集

デプロイメント・エディターの「システム・ビュー (System View)」ページを使用して、管理対象ホストを編集します。

始める前に

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、 171 ページの『NAT されたネットワーク』を参照してください。

NAT をサポートしないように構成されているコンソールに NAT された管理対象ホストを追加する場合、そのコンソールで NAT を無効にする必要があります。詳しくは、 173 ページの『管理対象ホストの NAT 状況の変更』を参照してください。

手順

1. 「システム・ビュー **(System View)**」タブをクリックします。
2. 編集する管理対象ホストを右クリックし、「管理対象ホストの編集 **(Edit Managed Host)**」を選択します。

   このオプションは、選択したコンポーネントに、QRadar の互換性のあるバージョンを実行している管理対象ホストがある場合のみに使用できます。
3. 「次へ」をクリックします。
4. 必要に応じてパラメーター値を編集します。

   以下の表を参照して、パラメーターを構成してください。

表 *49.* 管理対象ホストのパラメーター

パラメーター	説明
ホストを **NAT** する **(Host is NATed)**	この管理対象ホストで既存のネットワーク・アドレス変換 (NAT) を使用する場合に、このチェック・ボックスを選択します。
暗号化を有効にする **(Enable Encryption)**	ホストの SSH 暗号化トンネルを作成する場合に、このチェック・ボックスを選択します。
	2 つの管理対象ホスト間でデータ圧縮を有効にする場合に、このチェック・ボックスを選択します。

5. 「ホストを **NAT** する **(Host is NATed)**」チェック・ボックスを選択した場合は、パラメーターを構成します。

表 50. NAT されたネットワークのパラメーター

パラメーター	説明
追加するサーバーまたはアプライアンスのパブリック **IP** を入力 **(Enter public IP of the server or appliance to add)**	管理対象ホストはこの IP アドレスを使用して、NAT を使用するさまざまなネットワークで他の管理対象ホストと通信します。
NAT されたネットワークの選択 **(Select NATed network)**	管理対象ホストがコンソールと同じサブネットにある場合、NAT されたネットワークのコンソールを選択します。 管理対象ホストがコンソールと同じサブネットにない場合、NAT されたネットワークの管理対象ホストを選択します。

6. 「次へ」をクリックします。
7. 「終了」をクリックします。

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。QRadar コンソールをホスティングする管理対象ホストを削除することはできません。

ヒント**:** 「ホストの削除 **(Remove host)**」オプションは、選択したコンポーネントに、QRadar の互換性のあるバージョンを実行している管理対象ホストがある場合のみに使用できます。

手順

1. 「システム・ビュー **(System View)**」タブをクリックします。
2. 削除する管理対象ホストを右クリックし、「ホストの削除 **(Remove host)**」を選択します。
3. 「**OK**」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。

管理対象ホストの構成

デプロイメント・エディターの「システム・ビュー (System View)」ページを使用して、管理対象ホストを構成します。

手順

1. 「システム・ビュー (System View)」ページで、構成する管理対象ホストを右クリックし、「構成」をクリックします。
2. 以下のパラメーターの値を入力します。

「除外するポート **(Ports to exclude)**」フィールドで、コンマを使用して複数のポートを区切ります。

3. 「保存」をクリックします。

ホストへのコンポーネントの割り当て

「システム・ビュー (System View)」ページを使用して、「イベント・ビュー (Event View)」ページで追加した QRadar コンポーネントをデプロイメントの管理対象ホストに割り当てます。

ヒント**:** リスト・ボックスには、QRadar の互換性のあるバージョンを実行している管理対象ホストのみが表示されます。

手順

1. 「システム・ビュー **(System View)**」タブをクリックします。
2. 「管理対象ホスト」リストから、QRadar コンポーネントの割り当て先となる管理対象ホストを選択します。
3. 管理対象ホストに割り当てるコンポーネントを選択します。
4. メニューから、「アクション」 **>** 「割り当て」を選択します。
5. 「ホストの選択 **(Select a host)**」リスト・ボックスから、このコンポーネントに割り当てるホストを選択します。「次へ」をクリックします。
6. 「終了」をクリックします。

ホスト・コンテキストの構成

デプロイメント・エディターの「システム・ビュー (System View)」ページを使用して、管理対象ホストのホスト・コンテキスト・コンポーネントを構成します。

ホスト・コンテキスト・コンポーネントはすべての QRadar コンポーネントをモニターして、各コンポーネントが期待どおりに機能していることを確認します。

手順

1. デプロイメント・エディターで、「システム・ビュー **(System View)**」タブをクリックします。
2. 構成するホスト・コンテキストを含む管理対象ホストを選択します。
3. ホスト・コンテキスト・コンポーネントを選択します。
4. 「アクション」 > 「構成」をクリックします。
5. パラメーターの値を入力します。

表 51. 「ホスト・コンテキスト *(Host Context)*」のパラメーター

パラメーター	説明
警告しきい値 **(Warning Threshold)**	ディスク使用量の構成済みしきい値を超過すると、ディスク使用量の現在の状況を示す E メールが管理者に送信されます。 警告のデフォルトしきい値は 0.75 です。したがって、ディスク使用量が 75% を超えると、ディスク使用量が 75% を超えていることを示す E メールが送信されます。 ディスク使用量が増え続け、構成済みのしきい値を超えると、使用量が 5% 増えるたびに新しい E メールが送信されます。デフォルトで、ホスト・コンテキストは以下のパーティションでディスク使用量をモニターします。 • / • /store • /store/tmp **注:** 「アラート **E** メールの送信元アドレス」パラメーターに指定された E メール・アドレスから、「管理用 **E** メール・アドレス」パラメーターに指定された E メール・アドレスに通知 E メールが送信されます。これらのパラメーターは、「システム設定」ウィンドウで構成されます。詳しくは、 75 ページの『第 6 章 QRadarのセットアップ』を参照してください。
リカバリーしきい値 **(Recovery Threshold)**	システムがシャットダウンしきい値を超過した場合に処理を再開するには、ディスク使用量がリカバリーしきい値を下回っていることが必要です。デフォルトは、0.90 です。そのため、ディスク使用量が 90% を下回るまで処理は再開されません。 **注:** 「アラート **E** メールの送信元アドレス」パラメーターに指定された E メール・アドレスから、「管理用 **E** メール・アドレス」パラメーターに指定された E メール・アドレスに通知 E メールが送信されます。これらのパラメーターは、「システム設定」ウィンドウで構成されます。詳しくは、 75 ページの『第 6 章 QRadarのセットアップ』を参照してください。

表 51. 「ホスト・コンテキスト (Host Context)」のパラメーター (続き)

パラメーター	説明
シャットダウンしきい値 **(Shutdown Threshold)**	システムがシャットダウンしきい値を超過すると、すべての処理が停止されます。システムの現在の状況を示す E メールが管理者に送信されます。デフォルトは 0.95 であるため、ディスク使用量が 95% を超えると、すべての処理は停止します。 **注:** 「アラート **E** メールの送信元アドレス」パラメーターに指定された E メール・アドレスから、「管理用 **E** メール・アドレス」パラメーターに指定された E メール・アドレスに通知 E メールが送信されます。これらのパラメーターは、「システム設定」ウィンドウで構成されます。 **注:** 詳しくは、 75 ページの『第 6 章 QRadarのセットアップ』を参照してください。
検査間隔 **(Inspection Interval)**	ディスク使用量を判別する頻度 (ミリ秒単位)。
検査間隔 **(Inspection Interval)**	SAR 出力を検査する頻度 (ミリ秒単位)。
アラート間隔 **(Alert Interval)**	しきい値を超過したことを通知する頻度 (ミリ秒単位)。
時間解決 **(Time Resolution)**	SAR 検査が実行される時間 (秒単位)。
検査間隔 **(Inspection Interval)**	ログ・ファイルをモニターする頻度 (ミリ秒単位)。
モニター対象の **SYSLOG** ファイル名 **(Monitored SYSLOG File Name)**	SYSLOG ファイルのファイル名。
アラート・サイズ **(Alert Size)**	ログ・ファイルからモニターする行の最大数。

6. 「保存」をクリックします。

の構成アキュムレーター

デプロイメント・エディターの「システム・ビュー (System View)」ページを使用して、管理対象ホストのアキュムレーター・コンポーネントを構成します。

アキュムレーター・コンポーネントは、管理対象ホストのイベント・プロセッサー・プログラムに対するデータ収集とアノマリ検出に役立ちます。アキュムレーター・コンポーネントは、ローカル・イベント・プロセッサー・プログラムからのイベントおよびフローのストリームの受信やデータベース・データの書き込みを行います。また、アノマリ検出エンジン (ADE) が含まれています。

手順

1. デプロイメント・エディターで、「システム・ビュー **(System View)**」タブをクリックします。
2. 構成する管理対象ホストを選択します。

3. アキュムレーター・コンポーネントを選択します。
4. 「アクション」 > 「構成」をクリックします。
5. パラメーターを構成します。

表 52. アキュムレーターのパラメーター

パラメーター	説明
中央アキュムレーター **(Central Accumulator)**	現在のコンポーネントが中央アキュムレーターであるかどうかを指定します。中央アキュムレーターはコンソール・システムにのみ存在します。
アノマリ検出エンジン **(Anomaly Detection Engine)**	ADE はネットワーク・データを分析し、データをルールシステムに転送して解決します。 中央アキュムレーターの場合、以下の構文を使用してアドレスとポートを入力します。 *<Console>:<port>* 非中央アキュムレーターの場合、以下の構文を使用してアドレスとポートを入力します。 *<non-Console IP Address>:<port>*
ストリーマー・アキュムレーターの **listen** ポート **(Streamer Accumulator Listen Port)**	イベント・プロセッサー・プログラムからフローのストリームを受信する listen ポート。 デフォルト値は 7802 です。
アラート用 **DSM** アドレス **(Alerts DSM Address)**	アキュムレーターからアラートを転送するのに使用するデバイス・システム・モジュール (DSM) アドレス。 使用する構文は、*<DSM_IP address>:<DSM port number>* です。

6. 「保存」をクリックします。

NAT されたネットワーク

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。

Any 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。

これらの NAT グループのいずれかに、外部変換を必要としないホストがある場合、「プライベート **IP (Private 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 アドレスを入力します。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 アドレスおよび 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 されたネットワークの QRadar への追加

デプロイメント・エディターを使用して、NAT されたネットワークを QRadar のデプロイメント環境に追加します。

始める前に

静的 NAT 変換を使用して、NAT されたネットワークをセットアップしてください。このセットアップにより、各種の NAT されたネットワーク内に存在する管理対象ホスト間で通信できるようになります。

手順

1. デプロイメント・エディターで、「**NAT** されたネットワーク **(NATed Networks)**」アイコンをクリックします。
2. 「追加」をクリックします。
3. NAT に使用するネットワークの名前を入力します。
4. 「**OK**」をクリックします。

   「NAT されたネットワークの管理 (Manage NATed Networks)」ウィンドウが表示されます。追加したネットワークが NAT されたネットワークとして表示されています。
5. 「**OK**」をクリックします。
6. 「はい」をクリックします。

NAT されたネットワークの編集

デプロイメント・エディターを使用して、NAT されたネットワークを編集できます。

手順

1. デプロイメント・エディターで、「**NAT** されたネットワーク **(NATed Networks)**」アイコンをクリックします。

2. 編集する NAT されたネットワークを選択して、「編集」をクリックします。
3. NAT されたネットワークの新しい名前を入力して、「**OK**」をクリックします。

   「NAT されたネットワークの管理 (Manage NATed Networks)」ウィンドウに、更新済みの NAT されたネットワークが示されます。
4. 「**OK**」をクリックします。
5. 「はい」をクリックします。

NAT されたネットワークの QRadar からの削除

デプロイメント・エディターを使用して、NAT されたネットワークをデプロイメント環境から削除します。

手順

1. デプロイメント・エディターで、「**NAT** されたネットワーク **(NATed Networks)**」アイコンをクリックします。
2. 削除対象の、NAT されたネットワークを選択します。
3. 「削除」をクリックします。
4. 「**OK**」をクリックします。
5. 「はい」をクリックします。

管理対象ホストの NAT 状況の変更

デプロイメント・エディターを使用して、デプロイメントの管理対象ホストの NAT 状況を変更します。

始める前に

管理対象ホストに対して NAT を有効にする場合、NAT されたネットワークで静的 NAT 変換が使用されている必要があります。

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、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、そのホストに変更をデプロイできます。

手順

1. デプロイメント・エディターで、「システム・ビュー **(System View)**」タブをクリックします。
2. 編集する管理対象ホストを右クリックし、「管理対象ホストの編集 **(Edit Managed Host)**」を選択します。
3. 「次へ」をクリックします。
4. 次のオプションのいずれかを選択してください。
   - 管理対象ホストに対して NAT を有効にするには、「ホストを **NAT** する **(Host is NATed)**」チェック・ボックスを選択し、「次へ」をクリックします。

- 管理対象ホストに対して NAT を無効にするには、「ホストを **NAT** する **(Host is NATed)**」チェック・ボックスをクリアします。

重要**:** 既存の管理対象ホストの NAT 状況を変更すると、エラー・メッセージが表示される場合があります。そのようなエラー・メッセージは無視してください。

5. NAT を有効にした場合は、NAT されたネットワークを選択して、以下のパラメーターの値を入力します。

表 *53. NAT* されたネットワークのパラメーター

パラメーター	説明
追加するサーバーまたはアプライアンスのパブリック **IP** の変更 **(Change public IP of the server or appliance to add)**	管理対象ホストはこの IP アドレスを使用して、NAT を使用する別のネットワークに属する別の管理対象ホストと通信します。
NAT されたネットワークの選択 **(Select NATed network)**	NAT されたネットワーク構成を更新します。
NAT リストの管理 **(Manage NATs List)**	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、デプロイメントのセキュリティーを強化できます。 詳しくは、 171 ページの『NAT されたネットワーク』を参照してください。

6. 「次へ」をクリックします。
7. 「終了」をクリックします。
8. 管理対象ホストが通信するデバイス (ファイアウォール) の構成を更新します。
9. 「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。

コンポーネント構成

デプロイメント・エディターを使用して、デプロイメント内の各コンポーネントを構成します。

QRadar QFlow Collector の構成

デプロイメント・エディターを使用して、QRadar QFlow Collector を構成します。

このタスクについて

QRadar QFlow Collector および複数のQRadar Event Collectorから、接続に対してフロー・フィルターを構成できます。フロー・フィルターは、コンポーネントがどのフローを受信するかを制御します。「フロー・フィルター **(Flow Filter)**」パラメーターは、「フロー接続の構成 (Flow Connection Configuration)」ウィンドウで使用できます。

フロー・フィルタリングの対象として構成するコンポーネント間の矢印を右クリックして、「構成」を選択します。

以下の表には、QRadar QFlow Collector の拡張パラメーターが説明されています。

手順

1. 「イベント・ビュー (Event View)」または「システム・ビュー (System View)」ページから、構成する QRadar QFlow Collector を選択します。
2. 「アクション」 > 「構成」をクリックします。
3. 以下のパラメーターの値を入力します。

パラメーター	説明
イベント・コレクター接続 (Event Collector Connections)	この QRadar QFlow Collector に接続されているイベント・コレクター・コンポーネント。接続は、*<Host IP Address>:<Port>* の形式で表示されます。 QRadar QFlow Collector が イベント・コレクターに接続されていない場合、パラメーターは空になります。
QFlow Collector ID	QRadar QFlow Collector 固有の ID。
最大コンテンツ・キャプチャー (Maximum Content Capture)	フローに添付するキャプチャーの長さ (バイト単位)。範囲は 0 から 65535 までです。0 の値を指定すると、コンテンツ・キャプチャーは無効になります。デフォルトは、64 バイトです。 QRadar QFlow Collectorは、各フローの開始時に構成可能なバイト数をキャプチャーします。ネットワーク全体にわたって大量のコンテンツを転送すると、ネットワークおよびパフォーマンスに影響が及ぶ可能性があります。QRadar QFlow Collectorが閉じた高速リンクに配置されている管理対象ホスト上で、コンテンツ・キャプチャーの長さを増やすことができます。 **重要:** コンテンツ・キャプチャーの長さを増やすと、推奨されるディスク割り当てのディスク・ストレージ要件も増えます。

パラメーター	説明
別名自動検出 (Alias Autodetection)	「はい」オプションは、QRadar QFlow Collector が外部フロー・ソース別名を検出できるようにします。QRadar QFlow Collector 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 Collector は DNS リバース・ルックアップを試行して、デバイスのホスト名を決定しようとします。ルックアップに成功すると、QRadar QFlow Collector はこの情報をデータベースに追加し、すべてのデプロイメントにこの情報を報告します。 「いいえ」オプションは、QRadar QFlow Collector が外部フロー・ソース別名を検出しないようにします。

4. ツールバーで、「拡張」をクリックし、拡張パラメーターを表示します。
5. 必要に応じて、拡張パラメーターの値を入力します。

表 *54. QRadar QFlow Collector* の拡張パラメーター

パラメーター	説明
イベント・コレクター接続 (Event Collector Connections)	この QRadar QFlow Collector に接続されているイベント・コレクター。 接続は、*<Host IP Address>:<Port>* の形式で表示されます。 QRadar QFlow Collector が イベント・コレクターに接続されていない場合、パラメーターは空になります。
フロー・ルーティング・モード (Flow Routing Mode)	「**0**」オプションは、「ディストリビューター・モード **(Distributor Mode)**」が有効になり、QRadar QFlow Collector は類似するプロパティーを持つフローをグループ化できるようになります。 「**1**」オプションを指定すると、「フロー・モード **(Flow Mode)**」が有効になり、フローのバンドルが回避されます。
最大データ収集/パケット (Maximum Data Capture/Packet)	QRadar QFlow Collector に分析させるパケットごとのバイト数。
時間同期サーバー IP アドレス (Time Synchronization Server IP Address)	タイム・サーバーの IP アドレスまたはホスト名。
時間同期タイムアウト期間 (Time Synchronization Timeout Period)	タイムアウトになるまで管理対象ホストが時間同期を試行し続ける期間。 デフォルトは、15 分間です。

表 54. *QRadar QFlow Collector* の拡張パラメーター (続き)

パラメーター	説明
Endace DAG インターフェース・カード構成 (Endace DAG Interface Card Configuration)	Endace ネットワーク・モニター・インターフェース・カードのパラメーター。 このパラメーターで必要とされる入力データについて詳しくは、IBM サポート Web サイト (www.ibm.com/support) を参照してください。
フロー・バッファー・サイズ (Flow Buffer Size)	フロー・ストレージに予約するメモリー量 (MB 単位)。 デフォルトは 400 MB です。
フロー最大数 (Maximum Number of Flows)	QRadar QFlow Collector からイベント・コレクターに送信するフローの最大数。
重複フローの削除 (Remove duplicate flows)	「はい」オプションは、QRadar QFlow Collector が重複フローを削除できるようにします。 「いいえ」オプションは、QRadar QFlow Collector が重複フローを削除できないようにします。
NetFlow シーケンス番号の確認 (Verify NetFlow Sequence Numbers)	「はい」は、QRadar QFlow Collector が着信 NetFlow シーケンス番号をチェックして、すべてのパケットが確実に適切な順番で存在するようにします。 パケットが欠落しているか、間違った順番で受信されると、通知が表示されます。

表 54. *QRadar QFlow Collector* の拡張パラメーター (続き)

パラメーター	説明
外部フローの重複排除方法 (External Flow De-duplication method)	重複する外部フロー・ソースの削除 (重複排除) に使用する方法。 • 「ソース **(Source)**」は、QRadar QFlow Collector が元のフロー・ソースを比較できるようにします。 この方法では、特定のフローの最初の外部レコードをエクスポートしたデバイスの IP アドレスと、現在の外部フロー・レコードをエクスポートしたデバイスの IP アドレスが比較されます。IP アドレスが一致しない場合、現在の外部フロー・レコードは破棄されます。 • 「レコード **(Record)**」は、QRadar QFlow Collector が個々の外部フロー・レコードを比較できるようにします。 この方法では、特定のデバイスによって検出されたすべての外部フロー・レコードのリストがログに記録され、後続の各レコードとそのリストが比較されます。現在のレコードがリスト内に見つかった場合、そのレコードは破棄されます。
フロー・キャリー・オーバー期間 (Flow Carry-over Window)	フローの次の間隔が開始するまで、片側フローを保持する期間の終了までの秒数。 この設定により、レポートされる前に、フローの逆側が到着するまでの時間が計算に入れられます。

表 54. *QRadar QFlow Collector* の拡張パラメーター (続き)

パラメーター	説明
外部フロー・レコード比較マスク (External flow record comparison mask)	• このパラメーターは、「外部フローの重複排除方法 **(External Flow De-duplication method)**」パラメーターに「レコード **(Record)**」を入力した場合にのみ有効になります。 重複フローの削除に使用する外部フロー・レコード・フィールドには、以下のオプションが含まれます。 • **D** (方向) • **B** (バイト数) • **P** (パケット数) これらのオプションを組み合わせることができます。オプションの組み合わせとして使用可能な組み合わせは、以下のとおりです。 • 「**DBP**」オプションは、フロー・レコードを比較するときに、方向、バイト数、およびパケット数を使用します。 • 「**XBP**」オプションは、フロー・レコードを比較するときに、バイト数とパケット数を使用します。 • 「**DXP**」オプションは、フロー・レコードを比較するときに、方向とパケット数を使用します。 • 「**DBX**」オプションは、フロー・レコードを比較するときに、方向とバイト数を使用します。 • 「**DXX**」オプションは、フロー・レコードを比較するときに、方向を使用します。 • 「**XBX**」オプションは、フロー・レコードを比較するときに、バイト数を使用します。 • 「**XXP**」オプションは、フロー・レコードを比較するときに、パケット数を使用します。
スーパーフローの作成 (Create Superflows)	「はい」オプションは、QRadar QFlow Collector が、類似するプロパティーを持つグループ・フローからスーパーフローを作成できるようにします。 「いいえ」オプションは、スーパーフローが作成されないようにします。

表 54. *QRadar QFlow Collector* の拡張パラメーター (続き)

パラメーター	説明
タイプ A のスーパーフロー (Type A Superflows)	タイプ A のスーパーフローのしきい値。 タイプ A のスーパーフローは、1 つのホストから多数のホストへのフローのグループです。このフローは単一方向のフローであり、宛先ホストは異なっているが以下のパラメーターは同じであるすべてのフローを集約したものです。 • プロトコル • 送信元バイト数 • ソース・ホスト (Source hosts) • 宛先ネットワーク (Destination network) • 宛先ポート (Destination port) (TCP および UDP フローのみ) • TCP フラグ (TCP flags) (TCP フローのみ) • ICMP タイプ/コード (ICMP type, and code) (ICMP フローのみ)
タイプ B のスーパーフロー (Type B Superflows)	タイプ B のスーパーフローのしきい値。 タイプ B のスーパーフローは、多数のホストから 1 つのホストへのフローのグループです。このフローは単一方向のフローであり、異なる送信元ホストを持つが、以下のパラメーターは同じであるすべてのフローを集約したものです。 • プロトコル • 送信元バイト数 (Source bytes) • 送信元のパケット数 (Source packets) • 宛先ホスト (Destination host) • 送信元ネットワーク (Source network) • 宛先ポート (Destination port) (TCP および UDP フローのみ) • TCP フラグ (TCP flags) (TCP フローのみ) • ICMP タイプ/コード (ICMP type, and code) (ICMP フローのみ)

表 54. *QRadar QFlow Collector* の拡張パラメーター (続き)

パラメーター	説明
タイプ C のスーパーフロー (Type C Superflows)	タイプ C のスーパーフローのしきい値。 タイプ C のスーパーフローは、1 つのホストから別のホストへのフローのグループです。このフローは単一方向のフローであり、異なる送信元ポートまたは宛先ポートを持つが、以下のパラメーターは同じであるすべての非 ICMP フローを集約したものです。 • プロトコル • 送信元ホスト (Source host) • 宛先ホスト (Destination host) • 送信元バイト数 (Source bytes) • 宛先バイト数 (Destination bytes) • 送信元のパケット数 (Source packets) • 宛先のパケット数 (Destination packets)
非対称スーパーフローの再結合 (Recombine Asymmetric Superflows)	一部のネットワークでは、インバウンド・トラフィックとアウトバウンド・トラフィックで別々のパスを使用するようにトラフィックが構成されている場合があります。このルーティングを、非対称ルーティングといいます。1 つ以上の QRadar QFlow Collector から受信したフローを結合できます。ただし、複数の QRadar QFlow Collector コンポーネントからのフローを結合する場合は、QRadar QFlow Collector 構成の「非対称フロー・ソース・インターフェース **(Asymmetric Flow Source Interface(s))**」パラメーターでフロー・ソースを構成する必要があります。 • 「はい」オプションは、QRadar QFlow Collector が非対称フローを再結合できるようにします。 • 「いいえ」オプションは、QRadar QFlow Collector が非対称フローを再結合できないようにします。
非対称スーパーフローを無視 (Ignore Asymmetric Superflows)	「はい」オプションは、QRadar QFlow Collector が、非対称フローが有効な間にスーパーフローを作成できるようにします。 「いいえ」オプションは、QRadar QFlow Collector が、非対称フローが有効な間にスーパーフローを作成できないようにします。

表 54. *QRadar QFlow Collector* の拡張パラメーター (続き)

パラメーター	説明
最小バッファー・データ (Minimum Buffer Data)	収集されたデータが QRadar QFlow Collector プロセスに返されるまでに、Endace ネットワーク・モニター・インターフェース・カードが受け取る最小データ量 (バイト単位)。このパラメーターが 0 (ゼロ) で、使用可能なデータがない場合、Endace ネットワーク・モニター・インターフェース・カードは非ブロッキング振る舞いを許可します。
最大待機時間 (Maximum Wait Time)	Endace ネットワーク・モニター・インターフェース・カードが最小データ量を待機する最大時間 (マイクロ秒単位)。最小データ量は、「最小バッファー・データ **(Minimum Buffer Data)**」パラメーターで指定します。
ポーリング間隔 (Polling Interval)	Endace ネットワーク・モニター・インターフェース・カードが追加データのチェックを開始するまでに待機する期間 (マイクロ秒単位)。ポーリング間隔を設定するとカードへの過度なポーリング・トラフィックが回避されるため、帯域幅と処理時間が節約されます。

6. 「保存」をクリックします。
7. 構成するデプロイメント内のすべての QRadar QFlow Collectorに対して操作を繰り返します。

関連概念:

153 ページの『デプロイメント内の QRadar コンポーネントのイベント・ビュー』

イベント・コレクターの構成

デプロイメント・エディターを使用して、イベント・コレクターを構成します。

手順

1. 「イベント・ビュー (Event View)」または「システム・ビュー (System View)」ページから、構成するイベント・コレクターを選択します。
2. 「アクション」 > 「構成」をクリックします。
3. 次の各パラメーターの値を入力します。

パラメーター	説明
宛先イベント・プロセッサー・プログラム **(Destination Event Processor)**	このイベント・コレクターに接続されるイベント・プロセッサー・プログラム・コンポーネントを指定します。接続は、*<Host IP Address>:<Port>* の形式で表示されます。
フローの **listen** ポート **(Flow Listen Port)**	フローの listen ポート。

パラメーター	説明
イベント転送 **listen** ポート **(Event Forwarding Listen Port)**	イベント・コレクターのイベント転送ポート。
フロー転送 **listen** ポート **(Flow Forwarding Listen Port)**	イベント・コレクターのフロー転送ポート。

4. ツールバーで、「拡張」をクリックし、拡張パラメーターを表示します。
5. 必要に応じて、拡張パラメーターを構成します。

表 *55.* イベント・コレクターの拡張パラメーター

パラメーター	説明
プライマリー・コレクター **(Primary Collector)**	「**True**」の場合、イベント・コレクターがコンソール・システムに存在する、ということが指定されます。 「**False**」の場合、イベント・コレクターが非コンソール・システムに存在する、ということが指定されます。
自動検出の有効化 **(Autodetection Enabled)**	「はい」は、イベント・コレクターが、以前は不明であったログ・ソースからのトラフィックを自動的に分析して受け取れるようにします。該当するファイアウォール・ポートが開かれ、自動検出が有効になり、イベントが受信されます。このオプションはデフォルトです。 「いいえ」は、イベント・コレクターが、以前は不明であったログ・ソースからのトラフィックを自動的に分析したり、受け取ったりしないようにします。 詳しくは、「*Managing Log Sources Guide*」を参照してください。
フロー重複排除フィルター **(Flow Deduplication Filter)**	フローが転送されるまでにバッファーに入れられる期間 (秒単位)。
非対称フロー・フィルター **(Asymmetric Flow Filter)**	非対称フローが転送されるまでにバッファーに入れられる期間 (秒単位)。
既に検出されたイベントの転送 **(Forward Events Already Seen)**	「**True**」の場合、イベント・コレクターは、システムで検出されたイベントを転送できるようになります。 「**False**」の場合、イベント・コレクターは、システムで検出されたイベントを転送できなくなります。このオプションにより、システムでのイベント・ループが回避されます。

6. 「保存」をクリックします。
7. 構成するデプロイメント内のすべての QRadar Event Collectorに対して操作を繰り返します。

関連概念:

153 ページの『デプロイメント内の QRadar コンポーネントのイベント・ビュー』

イベント・プロセッサー・プログラムの構成

デプロイメント・エディターを使用して、イベント・プロセッサー・プログラムを構成します。

手順

1. 「イベント・ビュー (Event View)」または「システム・ビュー (System View)」ページから、構成するイベント・プロセッサー・プログラムを選択します。
2. 「アクション」 > 「構成」をクリックします。
3. 以下のパラメーターの値を入力します。

表 *56.* イベント・プロセッサー・プログラムのパラメーター値

パラメーター	説明
イベント・コレクター接続の **listen** ポート **(Event Collector Connections Listen Port)**	着信イベント・コレクター接続に対してイベント・プロセッサー・プログラムがモニターするポート。デフォルト値はポート 32005 です。
イベント・プロセッサー・プログラム接続の **listen** ポート **(Event Processor Connections Listen Port)**	着信イベント・プロセッサー・プログラム接続に対してイベント・プロセッサー・プログラムがモニターするポート。 デフォルト値はポート 32007 です。

4. ツールバーで、「拡張」をクリックし、拡張パラメーターを表示します。
5. 必要に応じて、パラメーターの値を入力します。

表 57. イベント・プロセッサー・プログラムの拡張パラメーター

パラメーター	説明
ルールのテスト **(Test Rules)**	「ルールのテスト **(Test Rules)**」リストは、非コンソール・イベント・プロセッサーでのみ使用可能です。ローカル側でテストするようにルールが構成されている場合、「グローバル **(Globally)**」オプションを使用してもルール設定はオーバーライドされません。 「ローカル **(Locally)**」を選択する場合、ルールはイベント・プロセッサー・プログラムでテストされ、システムとは共有されません。 「グローバル **(Globally)**」を選択する場合、各イベント・プロセッサー・プログラムの個々のルールをシステム全体で共有およびテストできます。表示される各ルールは、システム上のイベント・プロセッサー・プログラムが検出できるように「グローバル **(Global)**」に切り替えることができます。 例えば、5 分以内に 5 回ログインに失敗するとアラートが出されるルールを作成できます。ローカルルールを含むイベント・プロセッサー・プログラムで 5 回のログイン失敗が検出されると、ルールによって応答が生成されます。例のルールが「グローバル (Global)」に設定されている場合、いずれかのイベント・プロセッサー・プログラムで 5 分以内に 5 回ログインに失敗すると、ルールによって応答が生成されます。ルールがグローバルに共有されている場合、5 つのイベント・プロセッサー・プログラムから 1 回のログイン失敗が生じると、ルールによってそれが検出されます。 非コンソール・イベント・プロセッサー・プログラムではデフォルトでルールはグローバルにテストされ、イベント・プロセッサー・プログラムの各ルールはローカルでテストされるように設定されます。
オーバーフロー・イベント・ルーティングしきい値 **(Overflow Event Routing Threshold)**	イベント・プロセッサー・プログラムが管理できる 1 秒あたりのイベントのしきい値を入力します。このしきい値を超過したイベントはキャッシュに入れられます。
オーバーフロー・フロー・ルーティングしきい値 **(Overflow Flow Routing Threshold)**	イベント・プロセッサー・プログラムが管理できる 1 分あたりのフローのしきい値を入力します。このしきい値を超過したフローはキャッシュに入れられます。

表 57. イベント・プロセッサー・プログラムの拡張パラメーター (続き)

パラメーター	説明
イベント・データベース・パス **(Events database path)**	イベントを保存する場所を入力します。デフォルトは、**/store/ariel/events** です。
ペイロード・データベース長 **(Payloads database length)**	ペイロード情報を保存する場所。 デフォルトは、**/store/ariel/payloads** です。

6. 「保存」をクリックします。
7. 構成するデプロイメント内のすべての イベント・プロセッサーに対して操作を繰り返します。

関連概念:

153 ページの『デプロイメント内の QRadar コンポーネントのイベント・ビュー』

判定機能の構成

デプロイメント・エディターを使用して、判定機能コンポーネントを構成します。

手順

1. 「イベント・ビュー (Event View)」または「システム・ビュー (System View)」ページから、構成する判定機能を選択します。
2. 「アクション」 > 「構成」をクリックします。
3. ツールバーで、「拡張」をクリックし、拡張パラメーターを表示します。
4. 「オーバーフロー・ルーティングしきい値 **(Overflow Routing Threshold)**」フィールドで、判定機能がイベントを管理できる 1 秒あたりのイベントしきい値を入力します。

   このしきい値を超過したイベントはキャッシュに入れられます。

   デフォルトは、20,000 です。
5. 「保存」をクリックします。

関連概念:

153 ページの『デプロイメント内の QRadar コンポーネントのイベント・ビュー』

オフサイト・ソースの構成

デプロイメント・エディターを使用して、オフサイト・ソースを構成します。

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 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. 「イベント・ビュー (Event View)」または「システム・ビュー (System View)」ページから、構成するイベント・コレクターを選択します。
2. 「アクション」 > 「構成」をクリックします。
3. パラメーター値を入力します。

パラメーター	説明
イベントの受信 **(Receive Events)**	**True** - システムがオフサイト・ソース・ホストからイベントを受信できるようにします。 **False** - システムがオフサイト・ソース・ホストからイベントを受信しないようにします。
フローの受信 **(Receive Flows)**	**True** - システムがオフサイト・ソース・ホストからフローを受信できるようにします。 **False** - システムがオフサイト・ソース・ホストからフローを受信しないようにします。

4. 「保存」をクリックします。
5. 構成するデプロイメント内のすべてのオフサイト・ソースに対して操作を繰り返します。

関連概念:

153 ページの『デプロイメント内の QRadar コンポーネントのイベント・ビュー』

オフサイト・ターゲットの構成

デプロイメント・エディターを使用して、オフサイト・ターゲットを構成します。

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 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. 「イベント・ビュー (Event View)」または「システム・ビュー (System View)」ページから、構成するイベント・コレクターを選択します。
2. 「アクション」 > 「構成」をクリックします。
3. 以下のパラメーターの値を入力します。

パラメーター	説明
イベント・コレクター **listen** ポート **(Event Collector Listen Port)**	イベント・データを受信するための、イベント・コレクターの listen ポート。 イベントのデフォルト・ポートは 32004 です。
フロー・コレクターの **listen** ポート **(Flow Collector Listen Port)**	フロー・データを受信するための、イベント・コレクターの listen ポート。 フローのデフォルト・ポートは 32000 です。

4. 「保存」をクリックします。

関連概念:

153 ページの『デプロイメント内の QRadar コンポーネントのイベント・ビュー』

第 12 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 12 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

IBM Security QRadar アプライアンスの場合、IBM Security 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、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 Collector 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 Collector 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 Collector 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 Collector 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 Collector 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 Collector 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 SIEM を構成できます。QRadar SIEM 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。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 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。

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)

関連概念:

149 ページの『第 11 章 デプロイメント・エディター』
デプロイメント・エディターを使用して、QRadar の個々のコンポーネントを管理します。デプロイメントを構成した後、デプロイメントで各管理対象ホスト内の個々のコンポーネントにアクセスして、構成できます。

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 SIEM 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 SIEM 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 SIEM 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。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 Collector 構成について詳しくは、「*IBM Security QRadar SIEM* 管理ガイド」を参照してください。
- 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。
- 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 SIEM 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。
- 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 SIEM 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 QRadar QFlow Collector を構成していることを確認します。
- 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 デバイスからのクラス ID が QRadar QFlow Collector 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 SIEM 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 SIEM 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 SIEM 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 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 Collector 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 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 Collector 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 Collector 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。

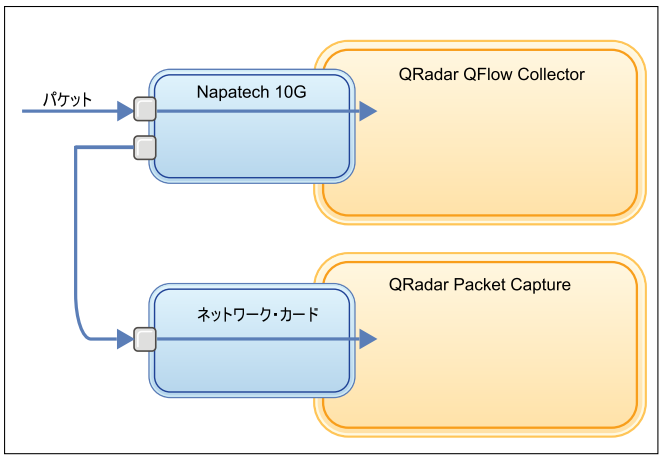

図 2. *Napatech* カードを使用して *QRadar QFlow Collector* から *QRadar Packet Capture* に転送されるパケット・データ

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 Collector 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. QRadar コンソールから、SSH を使用して root ユーザーとして QRadar QFlow Collector にログインします。QRadar QFlow Collector 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 Collector 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 QRadar サービスを再始動します。

   ```
   service hostcontext restart
   ```

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 Collector 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、QRadar Packet Capture の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 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 Collector 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 Collector 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 Collector 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 Collector 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 Collector コンポーネントにこの情報をレポートします。

デプロイメント・エディターを使用して、フロー・ソースの別名を自動的に検出するように QRadar QFlow Collector を構成します。

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 13 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。

デフォルトのリモート・ネットワーク・グループ

IBM Security QRadar SIEM 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 *58.* 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。
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/) を参照してください。

表 58. 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
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。
Neighbours	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。
TrustedNetworks	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	このグループは、デフォルトでブランクになっています。 このグループを構成して、モニターしたいネットワークから発生するトラフィックを分類することができます。

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。

デフォルトのリモート・サービス・グループ

IBM Security QRadar SIEM 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 59. 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。
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

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』
- 206 ページの『QID マップ・エントリーの変更』
- 207 ページの『Qid マップ・エントリーのインポート』
- 208 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 60. 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、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 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、「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 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。

オプション	説明
--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

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。

オプション	説明
--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

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 `.txt` ファイルにエクスポート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. 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。

第 14 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 SIEM* ユーザーズ・ガイド」を参照してください。

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 15 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。

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 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、ユーザー定義の表を対象にカスタム・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、75 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 (log source)
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。

また、ネットワーク階層ツールを使用して、事前構成されたドメインにネットワークを割り当てることもできます。詳しくは、 75 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」ルールでは、「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。

表 *61.* 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 61. 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 61. 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。キャプチャー結果では 4 人のユーザーのリストが返され、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、2 人のユーザーがドメイン A に割り当てられ、別の 2 人のユーザーがドメイン B に割り当てられています。

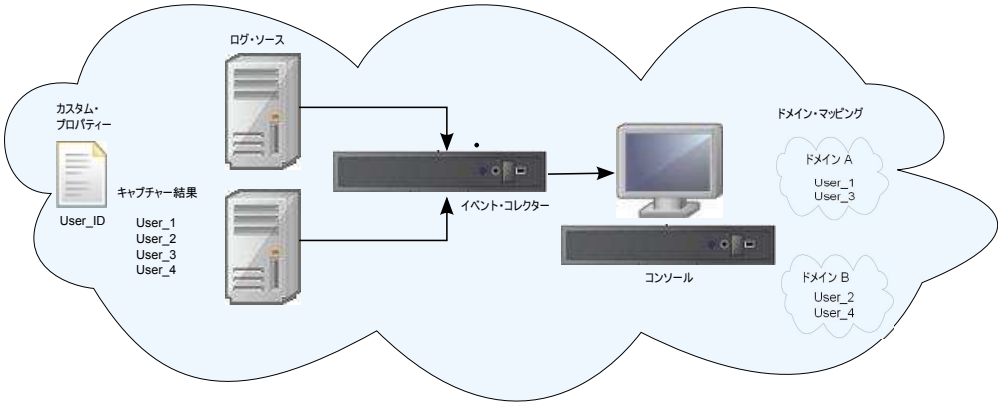

図 3. カスタム・イベント・プロパティーを使用したドメインの割り当て

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、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 16 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。

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) 管理者は以下のアクティビティーを担当します。

- 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 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、 226 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・ソースごとまたはドメインごとの 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、ログ・ソースおよびドメインの EPS レートが表示されます。

1. 「ネットワーク・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. ログ・ソースごとの EPS を表示するには、以下の照会を入力します。

```
select logsourcename(logsourceid) as LogSource, sum(eventcount) /
( ( max(endTime) - min(startTime) ) / 1000 ) as EPS from events
group by logsourceid order by EPS desc last 5 minutes
```

3. ドメインごとの EPS を表示するには、以下の照会を入力します。

```
select DOMAINNAME(domainid) as LogSource, sum(eventcount) /
( ( max(endTime) - min(startTime)) / 1000 ) as EPS from events
group by domainid order by EPS desc last 5 minutes
```

(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 *62.* 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、 211 ページの『第 15 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

「ネットワーク階層の定義 **(Define network hierarchy)**」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が、その変更をデプロイするには、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。

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。

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:

75 ページの『ネットワーク階層』

QRadar は、ネットワーク階層を使用してネットワーク・トラフィックを理解し、デプロイメント全体のアクティビティーを確認するための機能を提供します。

テナントの保存ポリシー

IBM Security QRadar デプロイメントの各テナントは、少なくとも 1 つのドメインを持ちます。ドメイン・フィルターを使用すると、マルチテナント・デプロイメントの場合の保存ポリシーを指定できます。

QRadar では、デプロイメントごとに最高 10 件の保存バケットがサポートされています。QRadar デプロイメントのテナントが 10 件以下の場合は、ドメイン・フィルターを使用して、カスタマーごとに別個のデータ保存ポリシーを作成することができます。

テナント固有の保存ポリシーを作成するには、テナント内の各ドメインにドメイン・ベースのフィルターを追加します。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、 104 ページの『データ保存』を参照してください。

第 17 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。

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**:** QRadar Log Manager では、QRadar Vulnerability Manager がインストールされている場合にのみアセット・データが追跡されます。IBM Security QRadar SIEM と IBM Security QRadar Log Manager の差異について詳しくは、5 ページの『ご使用のセキュリティー・インテリジェンス製品の機能』を参照してください。

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。ユーザーによって直接提供されるアセット更新は、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

このワークフローは、QRadar が、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判断する方法を示します。

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、既存のアセットと一致する IP アドレスが含まれているものの、既存のアセットとは一致しない別のアイデンティティー情報も含まれている場合、システムは他の情報を使用して、既存のアセットを更新する前にフォールス・ポジティブ一致を排除します。
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け取ると、システムはその更新の適用先のアセットを判別します。

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・データが提供されている場合、アセット・プロファイラーは以下の順序で情報の優先順位付けを行います。

- MAC アドレス (最も確定的である)
- NetBIOS ホスト名
- DNS ホスト名
- IP アドレス (最も低い優先度で決定)

MAC アドレス、NetBIOS ホスト名、および DNS ホスト名は固有でなければならないため、最も確実なアイデンティティー・データと見なされます。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、別個のブラックリストが備えられています。

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 *63.* 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
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

表 63. ルールのテストおよび対応 (続き)

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 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 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:

240 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:

249 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、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:

246 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。

247 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、IBM Security 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、 121 ページの『第 7 章 リファレンス・セット管理』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 *64.* 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*]
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・セットの処理について詳しくは、 121 ページの『第 7 章 リファレンス・セット管理』を参照してください。

関連概念:

242 ページの『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・セットの処理について詳しくは、 121 ページの『第 7 章 リファレンス・セット管理』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 *65.* 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*]

表 65. アセット・ホワイトリスト・データのリファレンス収集名 (続き)

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
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:

241 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 66. 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"`

表 66. 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 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"`

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 *67.* 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 Guide*」を参照してください。

関連概念:

243 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:

246 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 68. 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。
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 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. 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 18 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。

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 69. 「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	• **TCP** 正規化されたデータを送信するには、「**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。 • **UDP**
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	元の syslog メッセージに有効な syslog ヘッダーがない場合は、このチェック・ボックスを選択します。前に付加される syslog ヘッダーには、syslog ヘッダーの「ホスト名」フィールドの発信元ログ・ソース・デバイスの IP アドレス (IP アドレス・スプーフィング) が含まれます。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転送先を指定できます。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 *70.* 「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。

表 70. 「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
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・プログラムを指定します。 **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 70. 「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、データをデータベースに保管しないこと、CRE をバイパスすること、およびイベントを除去す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。 • 「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存されず、CRE によって処理されます。 • 「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。 すべてのイベントは、EPS ライセンスの対象としてカウントされます。

手順

1. 「管理」タブをクリックします。
2. ナビゲーション・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「ユーザーズ・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 71. 「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 19 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・プログラム・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 Hardware Guide*」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・プログラムも組み込まれていません。デフォルトでは、専用イベント・コレクターは、「デプロイメント・エディター」を使用して接続する必要があるイベント・プロセッサー・プログラムにイベントを継続的に転送します。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。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・プログラム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・プログラム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。

ストア・アンド・フォワードの概要

ストア・アンド・フォワード機能は、イベント・コレクター 1501 アプライアンスとイベント・コレクター 1590 アプライアンス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 Hardware Guide*」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・プログラムも組み込まれていません。デフォルトでは、専用イベント・コレクターは、デプロイメント・エディターを使用して接続する必要があるイベント・プロセッサー・プログラムにイベントを継続的に転送します。ストア・アンド・フォワード機能により、イベント・コレクターが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ていない間は、ローカルのアプライアンスにイベントが保管されるため、コンソールのユーザー・インターフェースを使用してイベントにアクセスすることはできません。

このスケジューリング機能により、業務時間内にイベントを保管し、送信プロセッサーがネットワーク帯域幅に影響しない時間に、保管したイベントをイベント・プロセッサー・プログラムに転送することができます。例えば、業務時間外 (午前 0

時から 6 時までなど) にのみイベントをイベント・プロセッサー・プログラムに転送するように、イベント・コレクターを構成することができます。

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 **(Store and Forward)**」アイコンをクリックします。
4. 「ストア・アンド・フォワード (Store and Forward)」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 72. 「ストア・アンド・フォワード (*Store and Forward*)」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QRadar Event Collector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 (QRadar Event Collector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QRadar Event Collectorとの間の、親子関係の階層を表示します。
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・プログラムの名前を示します。 • 「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・プログラムの名前を示します。 • 「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。

表 72. 「ストア・アンド・フォワード (*Store and Forward*)」ウィンドウのパラメーター (続き)

パラメーター	説明
スケジュール名 (Schedule Name)	「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・プログラム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。
最後の状況 (Last Status)	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・コレクター上にローカルで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QRadar Event Collectorがないか、割り当てられているQRadar Event Collector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 (Forwarded Events)	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。

表 72. 「ストア・アンド・フォワード (*Store and Forward*)」ウィンドウのパラメーター (続き)

パラメーター	説明
残りのイベント (Remaining Events)	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。
平均イベント速度 (Average Event Rate)	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・プログラムに転送される平均速度を表示します。 **ヒント:** 「平均イベント速度」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。
現在のイベント速度 (Current Event Rate)	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・プログラムに転送される速度を表示します。 **ヒント:** 「現在のイベント速度」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 (Transfer Rate Limit)	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。

新規ストア・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・プログラム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QRadar Event Collector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・プログラムに接続されているようにしてください。イベント・コレクターとイベント・プロセッサー・プログラムの接続は、デプロイメント・エディターで構成します。

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、「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 **(Store and Forward)**」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・コレクターがデプロイメント環境に追加されていない可能性があります。その場合は、「デプロイメント・エディター」を使用してイベント・コレクターを追加してから作業を実行します。
   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。

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、QRadar Event Collector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 **(Store and Forward)**」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 **(Store and Forward)**」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。

スケジュールを削除すると、関連するQRadar Event Collectorにより、割り当てられているイベント・プロセッサー・プログラムに対するイベントの継続的な転送が再開されます。

第 20 章 コンテンツ・マネジメント

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。

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。

セキュリティー・コンテンツ・タイプ

QRadar コンテンツは以下のタイプにバンドルされています。

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ための新しいカスタム・イベント・プロパティーが含まれています。

セキュリティー・コンテンツ・パックは IBM Fix Central 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配布されるものではありません。

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 から QRadar 拡張をダウンロードして、「拡張の管理」ツールを使用してインストールすることができます。セキュリティー拡張は自動更新の一環として配布されるものではありません。

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、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 *73.* 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
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

表 73. 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・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 74. 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。
-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。

表 74. 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
-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 75. 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

表 75. 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 (続き)

カスタム・コンテンツのタイプ	テキスト ID	数値 ID
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 76. 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、 279 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、 275 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 77. 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。

表 77. 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 (続き)

パラメーター	説明
-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、 275 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 78. 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。

表 78. 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
-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。
-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。

表 78. 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
-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 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、 284 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 79. 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、『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 80. 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
     ```

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、 275 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 *81.* 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
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 *82. 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。
-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。

表 82. *contentManagement.pl* スクリプト・パラメーター (続き)

パラメーター	説明
-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。
-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。

表 82. *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]*	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。
-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 21 章 SNMP トラップ構成

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。

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 83. 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 84. 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>
[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 85. *<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 *86. <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 22 章 データ難読化による機密データの保護

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。

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、 9 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 87. 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 88. 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 23 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、 55 ページの『ログ・ファイルの収集』を参照してください。

監査ログ

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 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 89. 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 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。

高可用性

- ライセンス・キーを追加する。

- ライセンスを戻す。
- ライセンス・キーを削除する。

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。

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 24 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関連する重大度レベルが含まれます。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。

上位イベント・カテゴリー

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。

着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 *90.* 上位イベント・カテゴリー

カテゴリー	説明
312 ページの『スキャン行為』	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)
314 ページの『DoS』	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)。
317 ページの『認証』	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)。
325 ページの『アクセス』	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)。
327 ページの『エクスプロイト (Exploit)』	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)。
329 ページの『マルウェア』	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。

表 90. 上位イベント・カテゴリー (続き)

カテゴリー	説明
330 ページの『疑わしいアクティビティー』	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。
335 ページの『システム』	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。
340 ページの『ポリシー』	企業のポリシー違反または誤用に関するイベント。
341 ページの『不明』	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。
342 ページの『CRE』	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。
342 ページの『潜在的エクスプロイト』	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。
344 ページの『ユーザー定義』	ユーザー定義オブジェクトに関連したイベント。
346 ページの『SIM 監査』	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。
347 ページの『VIS ホスト・ディスカバリー』	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。
348 ページの『アプリケーション』	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。
372 ページの『監査』	監査アクティビティーに関連したイベント。
373 ページの『リスク』	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。
374 ページの『リスク・マネージャー監査』	IBM Security QRadar Risk Manager の監査アクティビティーに関連したイベント。
375 ページの『制御』	ハードウェア・システムに関連したイベント。
377 ページの『アセット・プロファイラー』	アセット・プロファイル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 *91.* 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	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)	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)	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)	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)	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)	メール・システムのスキャン行為。	3
Windows スキャン行為 (Windows Reconnaissance)	Windows オペレーティング・システムに対するスキャン行為。	3
ポート・マップ/RPC 要求	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)	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)	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)	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)	その他のスキャン行為イベント。	2
Web スキャン行為 (Web Reconnaissance)	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)	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)	ICMP トラフィックのスキャン行為。	3
UDP スキャン行為 (UDP Reconnaissance)	UDP トラフィックのスキャン行為。	3
SNMP スキャン行為 (SNMP Reconnaissance)	SNMP トラフィックのスキャン行為。	3
ICMP ホスト照会 (ICMP Host Query)	ICMP ホスト照会を示します。	3
UDP ホスト照会 (UDP Host Query)	UDP ホスト照会を示します。	3
NMAP スキャン行為 (NMAP Reconnaissance)	NMAP スキャン行為を示します。	3

表 91. 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	説明	重大度レベル (0 から 10 まで)
TCP スキャン行為 (TCP Reconnaissance)	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 (UNIX Reconnaissance)	UNIX ネットワークのスキャン行為。	3
FTP スキャン行為 (FTP Reconnaissance)	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 92. *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	説明	重大度レベル (0 から 10 まで)
不明な DoS 攻撃 (Unknown DoS Attack)	不明な DoS 攻撃を示します。	8
ICMP DoS	ICMP DoS 攻撃を示します。	9
TCP DoS	TCP DoS 攻撃を示します。	9
UDP DoS	UDP DoS 攻撃を示します。	9
DNS サービス DoS (DNS Service DoS)	DNS サービス DoS 攻撃を示します。	8
Web サービス DoS (Web Service DoS)	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)	メール・サーバー DoS 攻撃を示します。	8
分散型 DoS	分散型 DoS 攻撃を示します。	9
その他の DoS (Misc DoS)	その他の DoS 攻撃を示します。	8
UNIX DoS	UNIX DoS 攻撃を示します。	8
Windows DoS	Windows DoS 攻撃を示します。	8
データベース DoS (Database DoS)	データベース DoS 攻撃を示します。	8
FTP DoS	FTP DoS 攻撃を示します。	8
インフラストラクチャー DoS (Infrastructure DoS)	インフラストラクチャーへの DoS 攻撃を示します。	8

表 92. 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	説明	重大度レベル (0 から 10 まで)
Telnet DoS	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)	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)	高速 TCP DoS 攻撃を示します。	8
高速 UDP DoS (High Rate UDP DoS)	高速 UDP DoS 攻撃を示します。	8
高速 ICMP DoS (High Rate ICMP DoS)	高速 ICMP DoS 攻撃を示します。	8
高速 DoS (High Rate DoS)	高速 DoS 攻撃を示します。	8
中速 TCP DoS (Medium Rate TCP DoS)	中速 TCP 攻撃を示します。	8
中速 UDP DoS (Medium Rate UDP DoS)	中速 UDP 攻撃を示します。	8
中速 ICMP DoS (Medium Rate ICMP DoS)	中速 ICMP 攻撃を示します。	8
中速 DoS (Medium Rate DoS)	中速 DoS 攻撃を示します。	8
中速 DoS (Medium Rate DoS)	中速 DoS 攻撃を示します。	8
低速 TCP DoS (Low Rate TCP DoS)	低速 TCP DoS 攻撃を示します。	8
低速 UDP DoS (Low Rate UDP DoS)	低速 UDP DoS 攻撃を示します。	8
低速 ICMP DoS (Low Rate ICMP DoS)	低速 ICMP DoS 攻撃を示します。	8
低速 DoS (Low Rate DoS)	低速 DoS 攻撃を示します。	8
分散型高速 TCP DoS (Distributed High Rate TCP DoS)	分散型高速 TCP DoS 攻撃を示します。	8
分散型高速 UDP DoS (Distributed High Rate UDP DoS)	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)	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)	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)	分散型中速 TCP DoS 攻撃を示します。	8

表 92. *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	説明	重大度レベル **(0** から **10** まで**)**
分散型中速 UDP DoS (Distributed Medium Rate UDP DoS)	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)	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)	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)	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)	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)	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)	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)	高速 TCP スキャンを示します。	8
高速 UDP スキャン (High Rate UDP Scan)	高速 UDP スキャンを示します。	8
高速 ICMP スキャン (High Rate CMP Scan)	高速 ICMP スキャンを示します。	8
高速スキャン	高速スキャンを示します。	8
中速 TCP スキャン (Medium Rate TCP Scan)	中速 TCP スキャンを示します。	8
中速 UDP スキャン (Medium Rate UDP Scan)	中速 UDP スキャンを示します。	8
中速 ICMP スキャン (Medium Rate ICMP Scan)	中速 ICMP スキャンを示します。	8
中速スキャン	中速スキャンを示します。	8
低速 TCP スキャン (Low Rate TCP Scan)	低速 TCP スキャンを示します。	8
低速 UDP スキャン (Low Rate UDP Scan)	低速 UDP スキャンを示します。	8
低速 ICMP スキャン (Low Rate ICMP Scan)	低速 ICMP スキャンを示します。	8
低速スキャン (Low Rate Scan)	低速スキャンを示します。	8
VoIP DoS	VoIP DoS 攻撃を示します。	8
フラッディング (Flood)	フラッド攻撃を示します。	8

表 92. 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	説明	重大度レベル (0 から 10 まで)
TCP フラッド (TCP Flood)	TCP フラッド攻撃を示します。	8
UDP フラッド (UDP Flood)	UDP フラッド攻撃を示します。	8
ICMP フラッド (ICMP Flood)	ICMP フラッド攻撃を示します。	8
SYN フラッド (SYN Flood)	SYN フラッド攻撃を示します。	8
URG フラッド (URG Flood)	緊急 (URG) フラグをオンにしたフラッド攻撃を示します。	8
SYN URG フラッド (SYN URG Flood)	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)	SYN FIN フラッド攻撃を示します。	8
SYN ACK フラッド (SYN ACK Flood)	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 93. 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	説明	重大度レベル (0 から 10 まで)
不明な認証 (Unknown Authentication)	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)	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)	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)	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)	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)	特権のエスカレーションが失敗したことを示します。	3

表 93. 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	説明	重大度レベル (0 から 10 まで)
成功した特権のエスカレーション (Privilege Escalation Succeeded)	特権のエスカレーションが成功したことを示します。	1
成功したメール・サービスのログイン (Mail Service Login Succeeded)	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)	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)	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)	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)	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)	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)	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)	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)	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)	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
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)	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)	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)	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)	SSH ログインが成功したことを示します。	1

表 93. 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	説明	重大度レベル (0 から 10 まで)
失敗した SSH ログイン (SSH Login Failed)	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)	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)	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)	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)	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)	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
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)	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)	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)	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)	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)	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)	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)	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)	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)	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

表 93. 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	説明	重大度レベル (0 から 10 まで)
削除されたグループ・メンバー (Group Member Removed)	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)	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)	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)	グループが削除されたことを示します。	1
追加されたコンピューター・アカウント (Computer Account Added)	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)	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)	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)	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)	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)	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)	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)	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)	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)	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)	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
失敗した Samba ログイン (Samba Login Failed)	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)	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

表 93. 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	説明	重大度レベル (0 から 10 まで)
閉じられた認証サーバーのセッション (Auth Server Session Closed)	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)	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)	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)	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)	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)	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)	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)	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)	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
リモート・アクセスのログアウト (Remote Access Logout)	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)	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)	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)	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)	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)	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

表 93. 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	説明	重大度レベル (0 から 10 まで)
終了した管理セッション (Admin Session Finished)	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)	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)	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)	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)	VoIP セッションの開始を示します。	1
終了した VoIP セッション (VoIP Session Terminated)	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)	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)	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)	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)	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)	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)	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)	IKE エラー・メッセージを示します。	1
IKE 状況 (IKE Status)	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)	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)	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)	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)	RADIUS セッション状況メッセージを示します。	1

表 93. 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	説明	重大度レベル (0 から 10 まで)
失敗した RADIUS 認証 (RADIUS Authentication Failed)	RADIUS 認証障害を示します。	3
成功した RADIUS 認証 (RADIUS Authentication Successful)	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)	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)	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)	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)	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)	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)	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)	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)	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)	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)	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
成功したステーション関連付け (Station Association Succeeded)	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)	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)	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

表 93. 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	説明	重大度レベル (0 から 10 まで)
失敗したステーション再関連付け (Station Reassociation Failed)	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)	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)	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)	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)	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)	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)	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)	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
SA の作成 (Creating SA)	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)	証明書の不一致を示します。	3
資格情報の不一致 (Credentials Mismatch)	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)	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)	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)	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)	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)	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	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

表 93. 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	説明	重大度レベル (0 から 10 まで)
SFTP ログアウト (SFTP Logout)	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 94. 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	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)	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)	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)	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)	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)	その他の通信イベントを示します。	3
IPS の拒否 (IPS Deny)	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)	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)	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)	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	変換グループが見つからないことを示します。	2

表 94. 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	説明	重大度レベル (0 から 10 まで)
その他の権限 (Misc Authorization)	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)	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)	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)	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)	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)	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)	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)	セッションがリセットされたことを示します。	3
終了したセッション (Session Terminated)	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)	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)	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)	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)	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)	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)	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)	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)	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)	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

表 94. 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	説明	重大度レベル (0 から 10 まで)
許可されたデータベース・アクション (Database Action Allowed)	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)	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)	FTP アクションが許可されたことを示します。	1
拒否された FTP アクション (FTP Action Denied)	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)	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)	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)	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)	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

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 95. 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	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)	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)	バッファー・オーバーフローを示します。	9
DNS エクスプロイト (DNS Exploit)	DNS エクスプロイトを示します。	9
Telnet エクスプロイト (Telnet Exploit)	Telnet エクスプロイトを示します。	9
Linux エクスプロイト (Linux Exploit)	Linux エクスプロイトを示します。	9

表 95. 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	説明	重大度レベル (0 から 10 まで)
UNIX エクスプロイト (UNIX Exploit)	UNIX エクスプロイトを示します。	9
Windows エクスプロイト (Windows Exploit)	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)	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)	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)	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)	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)	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)	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)	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)	FTP エクスプロイトを示します。	9
RPC エクスプロイト (RPC Exploit)	RPC エクスプロイトを示します。	9
SNMP エクスプロイト (SNMP Exploit)	SNMP エクスプロイトを示します。	9
NOOP エクスプロイト (NOOP Exploit)	NOOP エクスプロイトを示します。	9
Samba エクスプロイト (Samba Exploit)	Samba エクスプロイトを示します。	9
データベース・エクスプロイト (Database Exploit)	データベース・エクスプロイトを示します。	9
SSH エクスプロイト (SSH Exploit)	SSH エクスプロイトを示します。	9
ICMP エクスプロイト (ICMP Exploit)	ICMP エクスプロイトを示します。	9
UDP エクスプロイト (UDP Exploit)	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)	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)	DHCP エクスプロイトを示します。	9

表 95. 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	説明	重大度レベル (0 から 10 まで)
リモート・アクセス・エクスプロイト (Remote Access Exploit)	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)	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)	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)	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)	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)	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)	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)	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)	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

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 96. 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	説明	重大度レベル (0 から 10 まで)
不明なマルウェア (Unknown Malware)	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)	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)	悪意のあるメール添付を示します。	6

表 96. 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	説明	重大度レベル (0 から 10 まで)
悪意のあるソフトウェア (Malicious Software)	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)	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)	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)	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)	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)	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
コンテンツ・スキャン (Content Scan)	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)	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)	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)	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)	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)	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)	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)	検疫アクション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 97. 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	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)	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)	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)	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)	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)	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	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)	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)	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)	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)	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)	不明な回避イベントを示します。	5
IP スプーフ (IP Spoof)	IP スプーフを示します。	5
IP フラグメント (IP Fragmentation)	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)	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)	IDS 回避を示します。	5
DNS プロトコル・アノマリ (DNS Protocol Anomaly)	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)	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)	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)	ルーティング・プロトコル・アノマリを示します。	3

表 97. 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	説明	重大度レベル (0 から 10 まで)
Web プロトコル・アノマリ (Web Protocol Anomaly)	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)	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)	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)	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)	情報漏えいを示します。	1
潜在的なメール脆弱性 (Potential Mail Vulnerability)	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)	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)	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)	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)	DNS サーバーの潜在的な脆弱性を示します。	4
潜在的な SMB 脆弱性 (Potential SMB Vulnerability)	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)	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)	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)	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)	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)	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)	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)	疑わしい ICMP アクティビティーを示します。	2

表 97. 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	説明	重大度レベル (0 から 10 まで)
潜在的な NFS 脆弱性 (Potential NFS Vulnerability)	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)	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)	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)	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)	潜在的な SNMP 脆弱性を示します。	4
正しくない TCP フラグの組み合わせ (Illegal CP Flag Combination)	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)	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)	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)	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)	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)	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)	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)	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)	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)	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

表 97. 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	説明	重大度レベル (0 から 10 まで)
悪意のある IP (Hostile IP)	既知の悪意のある IP アドレスの使用を示します。	4
監視リスト IP (Watch list IP)	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)	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)	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)	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)	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)	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)	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)	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)	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)	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)	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)	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)	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
疑わしい BGP アクティビティー (Suspicious BGP Activity)	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)	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)	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

表 97. 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	説明	重大度レベル (0 から 10 まで)
検出された不良デバイス (Rogue Device Detected)	不正なデバイスが検出されたことを示します。	5

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 98. 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	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)	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)	システムの再始動を示します。	1
システム構成	システム構成の変更を示します。	1
システム停止 (System Halt)	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)	サービス障害を示します。	6
システム状況 (System Status)	すべての情報イベントを示します。	1
システム・エラー (System Error)	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)	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)	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)	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)	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)	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)	ホスト・ポリシーの変更が成功したことを示します。	1

表 98. 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	説明	重大度レベル (0 から 10 まで)
成功したファイルの変更 (Successful File Modification)	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)	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)	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)	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)	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)	レジストリーの変更が失敗したことを示します。	1
失敗したホスト・ポリシーの変更 (Failed Host-Policy Modification)	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)	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)	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)	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)	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)	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)	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)	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)	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)	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)	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

表 98. 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	説明	重大度レベル (0 から 10 まで)
レジストリーの削除 (Registry Deletion)	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)	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)	ファイルが削除されたことを示します。	1
アンインストールされたアプリケーション (Application Uninstalled)	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)	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)	システム情報を示します。	3
システム処置の許可 (System Action Allow)	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)	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)	crontab メッセージを示します。	1
クーロン状況 (Cron Status)	crontab 状況メッセージを示します。	1
失敗したクーロン	crontab 失敗メッセージを示します。	4
成功したクーロン	crontab 成功メッセージを示します。	1
デーモン	デーモン・メッセージを示します。	1
デーモン状況	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)	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)	デーモン成功メッセージを示します。	1
カーネル (Kernel)	カーネル・メッセージを示します。	1
カーネル状況 (Kernel Status)	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)	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)	カーネル成功メッセージを示します。	1

表 98. 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	説明	重大度レベル (0 から 10 まで)
認証	認証メッセージを示します。	1
情報 (Information)	情報メッセージを示します。	2
通知 (Notice)	通知メッセージを示します。	3
警告 (Warning)	警告メッセージを示します。	5
エラー (Error)	エラー・メッセージを示します。	7
重要 (Critical)	重要なメッセージを示します。	9
デバッグ (Debug)	デバッグ・メッセージを示します。	1
メッセージ (Messages)	汎用メッセージを示します。	1
特権アクセス (Privilege Access)	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)	アラート・メッセージを示します。	9
緊急 (Emergency)	緊急メッセージを示します。	9
SNMP 状況 (SNMP Status)	SNMP 状況メッセージを示します。	1
FTP 状況 (FTP Status)	FTP 状況メッセージを示します。	1
NTP 状況 (NTP Status)	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)	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)	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)	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)	ホット・スタンバイ有効化の失敗を示します。	5
失敗したホット・スタンバイ無効化 (Hot Standby Disable Failed)	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)	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

表 98. 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	説明	重大度レベル (0 から 10 まで)
失われたホット・スタンバイ関連付け (Hot Standby Association Lost)	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)	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)	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)	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)	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)	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)	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)	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)	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)	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)	ライセンス・エラーを示します。	5
ライセンスの状況	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)	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)	サービスの中断が検出されたことを示します。	5
ライセンス超過 (License Exceeded)	ライセンスされた能力を超過したことを示します。	3
パフォーマンス状況 (Performance Status)	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)	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)	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 *99.* 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	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)	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)	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)	リモート・アクセス・ポリシー違反を示します。	2
IRC/IM ポリシー違反 (IRC/IM Policy Violation)	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)	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)	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)	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)	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)	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)	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)	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)	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)	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)	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)	IRC ポリシー違反を示します。	2

表 *99.* 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	説明	重大度レベル **(0** から **10** まで**)**
IM ポリシー違反 (IM Policy Violation)	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
VoIP ポリシー違反 (VoIP Policy Violation)	VoIP ポリシー違反を示します。	2
成功 (Succeeded)	ポリシー成功メッセージを示します。	1
失敗 (Failed)	ポリシー失敗メッセージを示します。	4

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 *100.* 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	説明	重大度レベル **(0** から **10** まで**)**
不明	不明なイベントを示します。	3
不明な Snort イベント (Unknown Snort Event)	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)	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)	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)	不明な HP TippingPoint イベントを示します。	3
不明な Windows 認証サーバー・イベント (Unknown Windows Auth Server Event)	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)	不明な Nortel イベントを示します。	3
保管 (Stored)	不明な保管イベントを示します。	3
振る舞い	不明な振る舞いイベントを示します。	3

表 *100.* 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	説明	重大度レベル **(0** から **10** まで**)**
しきい値 (Threshold)	不明なしきい値イベントを示します。	3
アノマリ (Anomaly)	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 *101. 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	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)	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)	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)	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)	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)	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 *102.* 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	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)	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)	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)	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)	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)	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 (Potential UNIX Exploit)	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)	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	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
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)	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)	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)	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)	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)	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

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 *103.* 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	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)	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)	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)	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)	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
カスタムの監視機能 2 (Custom Sentry 2)	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)	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)	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)	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)	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)	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)	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)	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)	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

表 *103.* 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	説明	重大度レベル **(0** から **10** まで**)**
カスタム・ポリシー (中) (Custom Policy Medium)	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)	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
カスタム・ポリシー 1 (Custom Policy 1)	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)	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)	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)	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)	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)	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)	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)	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)	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)	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)	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
カスタム・ユーザー (高) (Custom User High)	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)	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

表 *103.* 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	説明	重大度レベル **(0** から **10** まで**)**
カスタム・ユーザー 2 (Custom User 2)	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)	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)	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)	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)	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)	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)	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)	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、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 *104. 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	説明	重大度レベル **(0** から **10** まで**)**
SIM ユーザー認証 (SIM User Authentication)	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)	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

表 *104. 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 (続き)

下位イベント・カテゴリー	説明	重大度レベル **(0** から **10** まで**)**
SIM ユーザー処置 (SIM User Action)	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)	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)	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)	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)	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)	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)	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)	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 *105. 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	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)	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)	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

表 *105. 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 *(*続き*)*

下位イベント・カテゴリー	説明	重大度レベル **(0** から **10** まで**)**
ディスカバーされた新しい脆弱性 (New Vuln Discovered)	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)	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)	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 *106.* 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	説明	重大度レベル **(0** から **10** まで**)**
開かれたメール (Mail Opened)	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)	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)	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)	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)	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)	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)	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)	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)	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)	FTP 接続が開かれたことを示します。	1

表 106. 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	説明	重大度レベル (0 から 10 まで)
閉じられた FTP (FTP Closed)	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)	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)	FTP 接続が終了したことを示します。	4
拒否された FTP (FTP Denied)	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)	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)	FTP 接続がリダイレクトされたことを示します。	3
開かれた HTTP (HTTP Opened)	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)	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)	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)	HTTP 接続が終了したことを示します。	4
拒否された HTTP (HTTP Denied)	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)	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)	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)	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)	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)	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)	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)	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)	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)	HTTPS 接続が終了したことを示します。	4
拒否された HTTPS (HTTPS Denied)	HTTPS 接続が拒否されたことを示します。	4

表 106. 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	説明	重大度レベル (0 から 10 まで)
進行中の HTTPS (HTTPS In Progress)	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)	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)	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)	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)	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)	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)	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)	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)	SSH 接続が終了したことを示します。	4
拒否された SSH (SSH Denied)	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)	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)	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)	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)	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)	リモート・アクセス接続が終了したことを示します。	4
拒否されたリモート・アクセス (RemoteAccess Denied)	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)	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	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)	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)	VPN 接続が開かれたことを示します。	1

表 106. 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	説明	重大度レベル (0 から 10 まで)
閉じられた VPN (VPN Closed)	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)	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)	VPN 接続が終了したことを示します。	4
拒否された VPN (VPN Denied)	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)	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)	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)	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)	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)	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)	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)	RDP 接続がリセットされたことを示します。	3
終了した RDP (RDP Terminated)	RDP 接続が終了したことを示します。	4
拒否された RDP (RDP Denied)	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)	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)	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)	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)	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)	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)	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)	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)	ファイル転送接続が進行中であることを示します。	1

表 106. 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	説明	重大度レベル (0 から 10 まで)
遅延したファイル転送 (FileTransfer Delayed)	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)	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	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)	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)	DNS 接続が閉じられたことを示します。	1
リセットされた DNS (DNS Reset)	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)	DNS 接続が終了したことを示します。	5
拒否された DNS (DNS Denied)	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)	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)	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)	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)	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)	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)	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	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)	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)	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)	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)	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	データベース接続が閉じられたことを示します。	1
リセットされたデータベース (Database Reset)	データベース接続がリセットされたことを示します。	5

表 *106.* 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	説明	重大度レベル **(0** から **10** まで**)**
終了したデータベース (Database Terminated)	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)	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)	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)	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)	SMTP 接続が確立されたことを示します。	1
SMTP クローズ	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)	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)	SMTP 接続が終了したことを示します。	5
拒否された SMTP (SMTP Denied)	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)	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)	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)	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)	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)	許可サーバー接続が確立されたことを示します。	1
閉じられた許可 (Auth Closed)	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)	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)	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)	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)	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)	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)	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

表 106. 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	説明	重大度レベル (0 から 10 まで)
リダイレクトされた許可 (Auth Redirected)	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)	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)	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)	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)	P2P 接続が終了したことを示します。	4
拒否された P2P (P2P Denied)	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)	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)	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)	Web 接続が閉じられたことを示します。	1
リセットされた Web (Web Reset)	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)	Web 接続が終了したことを示します。	4
拒否された Web (Web Denied)	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)	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)	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)	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)	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)	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)	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)	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)	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)	VoIP 接続が終了したことを示します。	3

表 *106.* 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	説明	重大度レベル **(0** から **10** まで**)**
拒否された VoIP (VoIP Denied)	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)	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)	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)	VoIP 接続がリダイレクトされたことを示します。	3
開始された LDAP セッション (LDAP Session Started)	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)	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)	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)	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)	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)	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)	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)	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)	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)	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)	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)	AAA 認証が成功したことを示します。	1
失敗した IPSEC 認証 (IPSEC Authentication Failed)	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)	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)	IPSEC セッションが開始されたことを示します。	1

表 106. 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	説明	重大度レベル (0 から 10 まで)
終了した IPSEC セッション (IPSEC Session Ended)	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)	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)	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)	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)	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)	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)	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)	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)	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)	IM セッションが遅延したことを示します	3
リダイレクトされた IM セッション (IM Session Redirected)	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)	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)	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)	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)	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)	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)	WHOIS セッションが進行中であることを示します。	1

表 *106.* 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	説明	重大度レベル **(0** から **10** まで**)**
リダイレクトされた WHOIS セッション (WHOIS Session Redirected)	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)	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)	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)	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)	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
開かれた TN3270 セッション (TN3270 Session Opened)	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)	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)	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)	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)	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)	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)	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)	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)	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)	TFTP セッションが終了したことを示します。	3

表 106. 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	説明	重大度レベル (0 から 10 まで)
拒否された TFTP セッション (TFTP Session Denied)	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)	TFTP セッションが進行中であることを示します。	1
開かれた Telnet セッション (Telnet Session Opened)	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)	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)	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)	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)	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)	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)	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)	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)	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)	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)	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)	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)	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)	SSL セッションが終了したことを示します。	3
拒否された SSL セッション (SSL Session Denied)	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)	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)	Simple Network Management Protocol (SNMP) セッションが確立されたことを示します。	1

表 *106.* 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	説明	重大度レベル **(0** から **10** まで**)**
閉じられた SNMP セッション (SNMP Session Closed)	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)	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)	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)	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)	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)	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)	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)	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)	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)	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
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)	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)	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)	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)	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)	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

表 106. 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	説明	重大度レベル (0 から 10 まで)
開かれた RUSERS セッション (RUSERS Session Opened)	(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)	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)	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)	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)	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)	Rsh 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 Rsh セッション (Rsh Session Reset)	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)	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)	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)	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)	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)	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)	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)	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)	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)	RLOGIN セッションが進行中であることを示します。	1

表 *106.* 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	説明	重大度レベル **(0** から **10** まで**)**
開かれた REXEC セッション (REXEC Session Opened)	(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)	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)	REXEC 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 REXEC セッション (REXEC Session Terminated)	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)	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)	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)	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)	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)	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)	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)	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)	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)	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)	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)	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)	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)	NTP セッションが拒否されたことを示します。	3
進行中の NTP セッション (NTP Session In Progress)	NTP セッションが進行中であることを示します。	1

表 106. 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	説明	重大度レベル (0 から 10 まで)
開かれた NNTP セッション (NNTP Session Opened)	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)	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)	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)	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)	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)	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)	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)	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	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)	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)	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)	NFS セッションが進行中であることを示します。	1
開かれた NCP セッション (NCP Session Opened)	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)	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)	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)	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)	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)	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)	NetBIOS セッションが確立されたことを示します。	1

表 *106.* 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	説明	重大度レベル **(0** から **10** まで**)**
閉じられた NetBIOS セッション (NetBIOS Session Closed)	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)	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)	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)	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)	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)	MODBUS セッションが確立されたことを示します。	1
閉じられた MODBUS セッション (MODBUS Session Closed)	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)	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)	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)	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)	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)	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)	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)	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)	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)	LPD セッションが拒否されたことを示します。	3

表 106. 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	説明	重大度レベル (0 から 10 まで)
進行中の LPD セッション (LPD Session In Progress)	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	Lotus Notes セッションが確立されたことを示します。	1
Lotus Notes セッションのクローズ	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	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	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	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	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	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)	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)	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)	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)	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)	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)	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)	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)	IRC 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 IRC セッション (IRC Session Terminated)	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)	IRC セッションが拒否されたことを示します。	3

表 *106.* 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	説明	重大度レベル **(0** から **10** まで**)**
進行中の IRC セッション (IRC Session In Progress)	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)	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)	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)	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)	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)	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)	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)	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)	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)	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)	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)	Ident セッションが拒否されたことを示します。	3
進行中の Ident セッション (Ident Session In Progress)	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)	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)	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)	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)	ICCP セッションが終了したことを示します。	3

表 *106.* 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	説明	重大度レベル **(0** から **10** まで**)**
拒否された ICCP セッション (ICCP Session Denied)	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)	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	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	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	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	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	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	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	Gopher セッションが確立されたことを示します。	1
閉じられた Gopher セッション (Gopher Session Closed)	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)	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)	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)	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)	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)	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)	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)	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)	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)	GIOP セッションが拒否されたことを示します。	3

表 *106.* 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	説明	重大度レベル **(0** から **10** まで**)**
進行中の GIOP セッション (GIOP Session In Progress)	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)	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)	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)	Finger 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 Finger セッション (Finger Session Terminated)	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)	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)	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)	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)	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)	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)	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)	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)	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)	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)	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)	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)	Remote .NET セッションが進行中であることを示します。	1

表 106. 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	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	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)	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)	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)	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)	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)	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)	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)	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)	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)	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)	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)	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)	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
閉じられた DHCP セッション (DHCP Session Closed)	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)	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)	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)	DHCP リースが正常に取得されたことを示します	1

表 *106.* 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	説明	重大度レベル **(0** から **10** まで**)**
失敗した DHCP (DHCP Failure)	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)	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)	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)	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)	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)	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)	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)	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)	CUPS 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 CUPS セッション (CUPS Session Reset)	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)	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)	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)	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)	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)	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)	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)	Chargen セッションが終了したことを示します。	3

表 106. 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	説明	重大度レベル (0 から 10 まで)
拒否された Chargen セッション (Chargen Session Denied)	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)	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)	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)	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)	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)	DAP セッションが拒否されたことを示します。	3
DAP セッション状況 (DAP Session Status)	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)	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)	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)	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)	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)	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)	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)	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)	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)	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)	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)	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)	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)	ゲーム・セッションが終了したことを示します。	3

表 *106.* 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	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)	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)	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)	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)	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)	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)	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)	データ転送を示します。	3
データウェアハウジング (Data Warehousing)	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)	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)	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)	ファイル転送を示します。	2
ゲーム (Games)	ゲーム・アクティビティーを示します。	4
ヘルスケア (Healthcare)	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)	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)	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
レガシー (Legacy)	レガシー・アクティビティーを示します。	1
メール (Mail)	メール・アクティビティーを示します。	1
その他 (Misc)	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)	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	ネットワーク管理アクティビティーを示します。	

表 106. 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	説明	重大度レベル (0 から 10 まで)
P2P	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)	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)	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)	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)	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)	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	VoIP アクティビティーを示します。	1
Web	Web アクティビティーを示します。	1
ICMP	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 107. 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	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)	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)	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	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)	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)	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)	データ選択プロセスが検出されたことを示します。	1

表 107. 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	説明	重大度レベル (0 から 10 まで)
データ切り捨て (Data Truncation)	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)	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)	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)	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

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 108. 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	説明	重大度レベル (0 から 10 まで)
ポリシー公開	ポリシーの露出が検出されたことを示します。	5
コンプライアンス違反 (Compliance Violation)	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)	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)	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)	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)	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)	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)	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

表 *108.* 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	説明	重大度レベル **(0** から **10** まで**)**
暗号化されていないデータ・ストア (Un-Encrypted Data Store)	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)	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)	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
誤った構成のホスト (Mis-Configured Host)	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)	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)	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)	パスワードが存在しないことを示します。	7
不正行為 (Fraud)	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)	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)	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)	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)	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 *109.* 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	説明	重大度レベル **(0** から **10** まで**)**
ポリシー・モニター	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	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	シミュレーションが変更されたことを示します。	3
管理	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 *110.* 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	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)	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)	デバイスとの通信を示します。	1
デバイス監査 (Device Audit)	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)	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)	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)	デバイスが構成したことを示します。	1
デバイス・ルート (Device Route)	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)	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)	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)	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)	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

表 *110.* 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	説明	重大度レベル **(0** から **10** まで**)**
リレー・イベント (Relay Event)	リレー・イベントを示します。	1
NIC イベント (NIC Event)	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	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)	Integrated Management Unit (IMU) のイベントを示します。	1
請求イベント (Billing Event)	請求イベントを示します。	1
DBMS イベント (DBMS Event)	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)	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)	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)	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)	エクスポートが行われたことを示します。	1
リモート信号 (Remote Signalling)	リモート信号を示します。	1
ゲートウェイ状況 (Gateway Status)	ゲートウェイ状況を示します。	1
ジョブ・イベント (Job Event)	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)	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)	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)	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	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)	停電が発生したことを示します。	1
電力回復 (Power Restoration)	電力が回復したことを示します。	1
ハートビート (Heartbeat)	ハートビート ping が発生したことを示します。	1

表 *110.* 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	説明	重大度レベル **(0** から **10** まで**)**
リモート接続イベント (Remote Connection Event)	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 *111.* 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	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)	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)	アセットが更新されたことを示します。	1
監視されたアセット (Asset Observed)	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)	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)	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)	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)	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)	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)	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)	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)	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)	ポートがクリーンされたことを示します。	1

表 *111.* 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	説明	重大度レベル **(0** から **10** まで**)**
作成されたアセット・ポート (Asset Port Created)	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)	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)	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)	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)	ポー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脆弱性インスタンス (Asset Vuln Instance Cleaned)	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)	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)	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)	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)	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)	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)	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)	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)	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)	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)	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

表 *111.* 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	説明	重大度レベル **(0** から **10** まで**)**
削除されたアセット OS (Asset OS Deleted)	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
クリーンされたアセット・プロパティー (Asset Property Cleaned)	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)	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)	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)	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)	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)	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)	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)	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)	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)	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)	IP アドレスが移動されたことを示します。	1
削除されたアセット IP アドレス (Asset IP Address Deleted)	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)	インターフェースがクリーンされたことを示します。	1

表 *111.* 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	説明	重大度レベル **(0** から **10** まで**)**
作成されたアセット・インターフェース (Asset Interface Created)	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	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)	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)	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)	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	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)	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)	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)	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)	ユーザ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・スキャン・ポリシー (Asset Scanned Policy Cleaned)	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)	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)	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)	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)	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

表 *111.* 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	説明	重大度レベル **(0** から **10** まで**)**
監視されたアセット Windows アプリケーション (Asset Windows Application Observed)	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)	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)	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)	スキャン・サービス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・サービス (Asset Scanned Service Observed)	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)	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)	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)	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)	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)	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)	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)	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)	UNIX パッチが監視されたことを示します。	1

表 *111.* 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	説明	重大度レベル **(0** から **10** まで**)**
移動されたアセット UNIX パッチ (Asset UNIX Patch Moved)	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)	UNIX 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・パッチ・スキャン (Asset Patch Scan Cleaned)	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)	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	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)	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)	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	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)	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)	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)	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)	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
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)	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)	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

表 *111.* 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	説明	重大度レベル **(0** から **10** まで**)**
監視されたアセット・パッチ・スキャン (Asset Patch Scan Observed)	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)	ポート・スキャンが監視されたことを示します。	1

第 25 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・プログラム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 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。

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 *112. 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。
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)。

表 112. *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
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 QRadar Event Collector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 Collector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 112. *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 Collector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 Collector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。
161	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 Collector。	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。

表 112. *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 Collector。	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 Collector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 112. *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・プログラム・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 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 112. *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 112. *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。 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、 396 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・ホスト間のドライブの同期を保持する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。
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。

表 112. *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
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。
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。
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 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。
9999	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。このポートは、QVM が有効なときにのみ使用されます。

表 112. *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
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)。
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 Collector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 Collector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。

表 112. *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
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)。
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 で使用される一部のポートでは、追加のランダム・ポート番号が割り振られます。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 localhost 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、サービスには新しいポート番号のセットが提供されます。

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 localhost 7677
   ```
3. 何の情報も表示されない場合は、Enter キーを押して接続を閉じます。

QRadar が使用中のポートの検索

netstat コマンドを使用して、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 *113. 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。
www.iss.net	X-Force 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 *114. 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
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

表 *114. 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
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

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

以下の保証は、国または地域の法律に沿わない場合は、適用されません。

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 Corporation
170 Tracer Lane,
Waltham MA 02451, USA

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。

この文書に含まれるいかなるパフォーマンス・データも、管理環境下で決定されたものです。そのため、他の操作環境で得られた結果は、異なる可能性があります。一部の測定が、開発レベルのシステムで行われた可能性がありますが、その測定値が、一般に利用可能なシステムのものと同じである保証はありません。さらに、一部の測定値が、推定値である可能性があります。実際の結果は、異なる可能性があります。お客様は、お客様の特定の環境に適したデータを確かめる必要があります。

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。

この情報をソフトコピーでご覧になっている場合は、写真やカラーの図表は表示されない場合があります。

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。

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。

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。

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。

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。

プライバシー・ポリシーに関する考慮事項

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、[製品名] 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)**
ポジティブ (サイトが攻撃に対して脆弱であることを示す) として分類されるが、実際のユーザーの判断はネガティブ (脆弱ではない) となるテスト結果。

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 **(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 **(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 **(**サブネット**) (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

R

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