IBM Security QRadar

バージョン 7.2.6

インストール・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、 69 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。

本書は、本書の更新版に置き換えられない限り、IBM QRadar Security Intelligence Platform V7.2.6 および以降のリリースに適用されます。

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

原典： IBM Security QRadar
Version 7.2.6
Installation 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 のインストールの概要

IBM® Security QRadar® アプライアンスには、ソフトウェアおよび Red Hat Enterprise Linux オペレーティング・システムがプリインストールされています。ユーザーのハードウェアに QRadar ソフトウェアをインストールすることもできます。

IBM のアプライアンスをご注文いただき、ありがとうございます。最適な結果を得るために、最新のメンテナンスをアプライアンスに適用することを強くお勧めします。IBM Fix Central (http://www.ibm.com/support/fixcentral) にアクセスして、該当する製品の最新の推奨パッチを確認してください。

高可用性 (HA) システムをインストールまたはリカバリーするには、「*IBM Security QRadar High Availability Guide*」を参照してください。

対象読者

QRadar システムのインストールと構成を担当するネットワーク管理者は、ネットワーク・セキュリティーの概念と Linux オペレーティング・システムについて理解している必要があります。

技術資料

IBM Security QRadar の製品資料を Web で入手するには、IBM Knowledge Center (http://www.ibm.com/support/knowledgecenter/SS42VS/welcome) にアクセスしてください。各言語に翻訳された資料もすべて用意されています。

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

お客様サポートへのお問い合わせ

お客様サポートへのお問い合わせ方法については、Support and Download Technical Note (http://www.ibm.com/support/docview.wss?uid=swg21616144) を参照してください。

適切なセキュリティーの実践に関する注意事項

IT システムのセキュリティーでは、企業の内部と外部からの不正なアクセスの防止、検出、対応により、システムと情報を保護する必要があります。不正なアクセスにより、情報の改ざん、破壊、盗用、悪用が発生したり、使用しているシステムの損傷や、他のシステムに対する攻撃のための利用を含む悪用につながる可能性があります。完全に安全と見なすことができる IT システムまたは IT 製品は存在せず、また単一の製品、サービス、またはセキュリティー対策が、不適切な使用またはアクセスを防止する上で、完全に有効となることもありません。IBM のシステム、製品およびサービスは、合法かつ包括的なセキュリティーの取り組みの一部となるように設計されており、これらには必ず追加の運用手順が伴います。また、最

高の効果を得るために、他のシステム、製品、またはサービスを必要とする場合があります。IBM は、何者かの悪意のある行為または違法行為によって、システム、製品、またはサービスのいずれも影響を受けないこと、またはお客様の企業がそれらの行為によって影響を受けないことを保証するものではありません。

注意**:**

本プログラムの利用は、様々な法律または規制に関わる場合があります。これには、プライバシー、データ保護、雇用、電子通信、および電子保管に関連するものが含まれます。IBM Security QRadar は、合法的な目的のために合法的な手段を用いてのみ使用することができます。お客様は、適用される法律、規制、およびポリシーに従って本プログラムを使用することに同意し、かかる法律、規制、およびポリシーを遵守する全責任を負うものとします。ライセンシーは、IBM Security QRadar の合法的な使用に必要なすべての同意、許可、または使用権を取得するか、取得済みであることを表明するものとします。

第 1 章 QRadar のデプロイメントの概要

小規模の企業では IBM Security QRadar を単一サーバーにインストールし、大企業の環境では複数サーバーにインストールすることができます。

パフォーマンスとスケーラビリティーを最大限に引き出すため、高可用性 (HA) 保護が必要な各システムに対して HA 管理対象ホスト・アプライアンスをインストールする必要があります。 HA システムのインストールやリカバリーについて詳しくは、「*IBM Security QRadar High Availability Guide*」を参照してください。

アクティベーション・キーおよびライセンス・キー

IBM Security QRadar アプライアンスをインストールするときには、アクティベーション・キーを入力する必要があります。インストール後に、ライセンス・キーを適用する必要があります。インストール・プロセスで誤ったキーを入力しないようにするには、これらのキーの違いを理解しておくことが重要です。

アクティベーション・キー

アクティベーション・キーは、IBM から受け取る、4 つの部分に区切られた 24 桁の英数字ストリングです。すべての QRadar 製品のインストールでは同じソフトウェアを使用します。ただし、アクティベーション・キーによって、各アプライアンス・タイプに適用されるソフトウェア・モジュールが指定されます。例えば IBM Security QRadar QFlow コレクター のアクティベーション・キーを使用して QRadar QFlow コレクター モジュールのみをインストールします。

アクティベーション・キーは以下の場所から入手できます。

- QRadar ソフトウェアがプリインストールされているアプライアンスを購入した場合、同梱されている CD 上の文書にアクティベーション・キーが記載されています。
- QRadar ソフトウェアまたは仮想アプライアンスのダウンロード版を購入した場合、「始めに *(Getting Started)*」文書にアクティベーション・キーのリストが記載されています。「始めに *(Getting Started)*」は確認 E メールに添付されています。

ライセンス・キー

ご使用のシステムには、QRadar ソフトウェアに 5 週間アクセスできる一時ライセンス・キーが含まれています。ソフトウェアのインストール後、デフォルトのライセンス・キーが有効期限切れになるまでの間に、購入したライセンスを追加する必要があります。

デフォルトのライセンス・キーの制限を以下の表に示します。

表 *1. QRadar SIEM* のインストールでのデフォルト・ライセンス・キーの制限

使用	制限
アクティブ・ログ・ソース制限	750
1 秒当たりのイベントしきい値	5000

表 1. *QRadar SIEM* のインストールでのデフォルト・ライセンス・キーの制限 (続き)

使用	制限
間隔当たりのフロー	200000
ユーザー制限	10
ネットワーク・オブジェクト制限	300

表 2. *QRadar Log Manager* のインストールでのデフォルト・ライセンス・キーの制限

使用	制限
アクティブ・ログ・ソース制限	750
1 秒当たりのイベントしきい値	5000
ユーザー制限	10
ネットワーク・オブジェクト制限	300

QRadar 製品を購入すると、永続ライセンス・キーが記載されている E メールが IBM から送信されます。このライセンス・キーにより、ご使用のアプライアンス・タイプの機能が拡張され、システム操作パラメーターが定義されます。デフォルト・ライセンスが有効期限切れになる前に、ライセンス・キーを適用する必要があります。

関連タスク:

19 ページの『第 3 章 QRadar コンソールまたは管理対象ホストのインストール』
QRadar アプライアンスまたはユーザーのアプライアンスに、IBM Security QRadar コンソールまたは管理対象ホストをインストールします。

25 ページの『ユーザーのアプライアンスへの RHEL のインストール』
IBM Security QRadar で使用する Red Hat Enterprise Linux オペレーティング・システムをユーザーのアプライアンスにインストールできます。

33 ページの『仮想マシンでの QRadar ソフトウェアのインストール』
仮想マシンを作成したら、IBM Security QRadar ソフトウェアを仮想マシンにインストールする必要があります。

統合管理モジュール

各アプライアンス・タイプのバック・パネルにある統合管理モジュールを使用して、シリアル・コネクターとイーサネット・コネクターを管理します。

イーサネット・ポートを IBM Security QRadar 製品管理インターフェースと共有するように統合管理モジュールを構成できます。ただし、アプライアンスを再始動するときに接続が失われるリスクを低減するには、専用モードで統合管理モジュールを構成します。

統合管理モジュールを構成するには、IBM スプラッシュ画面が表示されたら F1 を押してシステム BIOS 設定にアクセスする必要があります。統合管理モジュールの構成について詳しくは、アプライアンスに付属の CD に収録されている統合管理モジュール ユーザーズ・ガイドを参照してください。

関連概念:

6 ページの『QRadar のインストールに関するハードウェア・アクセサリーおよびデスクトップ・ソフトウェアの前提条件』
IBM Security QRadar 製品をインストールする前に、必要なハードウェア・アクセサリーとデスクトップ・ソフトウェアにアクセスできることを確認してください。

QRadar コンポーネント

IBM Security QRadar は、ネットワーク上のデバイスやアプリケーションによって使用されるログ・ソースからのイベント・データを統合します。

重要: デプロイメントのすべての IBM Security QRadar アプライアンスのソフトウェア・バージョンのバージョンとフィックス・レベルが同一である必要があります。複数の異なるバージョンのソフトウェアを使用するデプロイメントはサポートされていません。

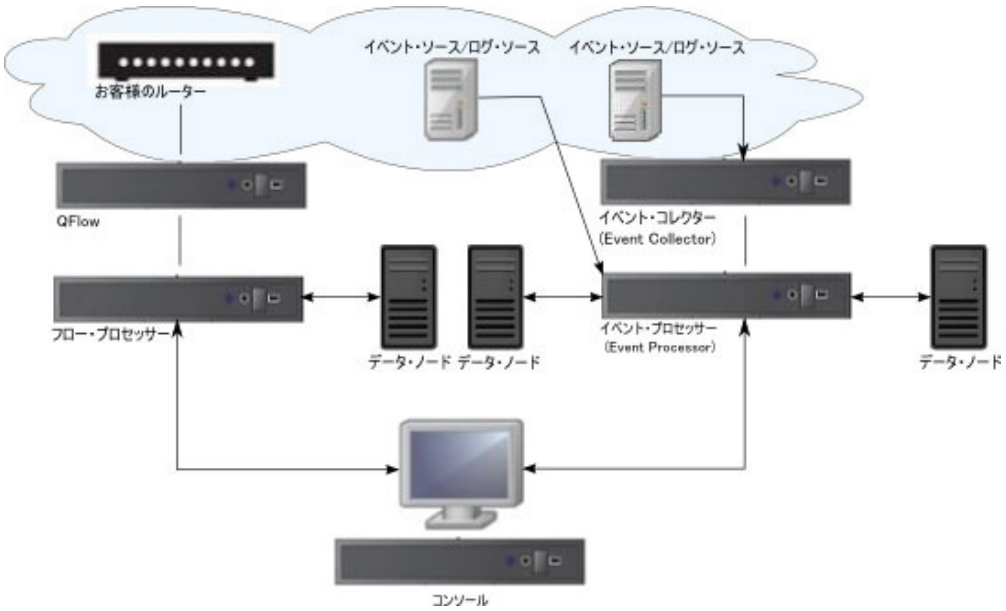

図 *1. QRadar* デプロイメント環境の例

QRadar デプロイメントには、以下のコンポーネントを組み込むことができます。

QRadar QFlow コレクター

スパン・ポートまたはネットワーク・タップを介してネットワークからトラフィック・フローをパッシブに収集します。IBM Security QRadar QFlow コレクター では、外部のフロー・ベースのデータ・ソース (NetFlow など) の収集もサポートされています。

QRadar QFlow コレクター をユーザーのハードウェアにインストールするか、または QRadar QFlow コレクター アプライアンスの 1 つを使用することができます。

制約事項: このコンポーネントは、QRadar SIEM デプロイメントに対してのみ使用できます。

QRadar コンソール

QRadar 製品のユーザー・インターフェースを提供します。インターフェースからリアルタイムのイベント・ビューとフロー・ビュー、レポート、オフェンス、アセット情報、管理機能が提供されます。

分散 QRadar デプロイメントでは、QRadar コンソールを使用して他のコンポーネントが含まれているホストを管理します。

判定機能

QRadar コンソール上で稼働するサービスである 判定機能 は、中核処理コンポーネントを提供します。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。判定機能では、ネットワーク・トラフィックとセキュリティー・イベントのビュー、レポート、アラート、および分析が提供されます。

判定機能コンポーネントは、カスタム・ルールと照合してイベントを処理します。イベントがルールと一致すると、判定機能コンポーネントにより、カスタム・ルールで構成されている応答が生成されます。

例えば、イベントがカスタム・ルールに一致するとオフェンスが作成されることを指定したカスタム・ルールがあるとします。カスタム・ルールと一致しない場合、判定機能コンポーネントはデフォルト・ルールを使用してイベントを処理します。オフェンスとは、複数の入力値、個々のイベント、および分析済みの振る舞いと脆弱性が結合されたイベントを使用して処理されるアラートです。判定機能コンポーネントによりオフェンスに優先順位が付けられ、いくつかの要因 (イベントの数、重大度、関連性、信頼性など) に基づいてマグニチュードの値が割り当てられます。

QRadar イベント・コレクター **(Event Collector)**

ローカルとリモートのログ・ソースからイベントを収集します。未加工のログ・ソース・イベントを正規化します。このプロセスでは、QRadar コンソール上の判定機能コンポーネントによってログ・ソースのイベントが検査され、イベントが QRadar ID (QID) にマップされます。その後、システムの使用を節減するためにイベント・コレクター (Event Collector)が同一イベントをバンドルし、その情報をイベント・プロセッサー (Event Processor) に送信します。

- WAN リンクが低速であるリモート・ロケーションでは QRadar Event Collector 1501 を使用します。イベント・コレクター (Event Collector)・アプライアンスは、イベントをローカルに保管しません。代わりに、これらのアプライアンスは、イベントを収集および解析した後で、保管するためにイベントをイベント・プロセッサー (Event Processor)・アプライアンスに送信します。
- イベント・コレクター (Event Collector)は、WAN の制限を回避するために、帯域幅リミッターとスケジュールを使用して、イベントをイベント・プロセッサー (Event Processor)に送信できます。
- イベント・コレクター (Event Collector)は、接続先のイベント・プロセッサー (Event Processor)と一致する EPS ライセンスに割り当てられます。

.

QRadar イベント・プロセッサー (Event Processor)

1 つ以上のイベント・コレクター (Event Collector)・コンポーネントから収集されたイベントを処理します。イベント・プロセッサー (Event Processor)は、QRadar 製品からの情報を相関付け、イベントのタイプに応じてその情報を該当するエリアに配布します。

イベント・プロセッサー (Event Processor)はまた、イベントのポリシー違反または振る舞い変更を示すため、QRadar 製品によって収集された情報を組み込みます。処理が完了すると、イベント・プロセッサー (Event Processor)はイベントを判定機能コンポーネントに送信します。

イベント・プロセッサーを追加する場合

- イベント速度が QRadar 3105 (All-in-One) のレーティング (5000 EPS) を超える場合は、QRadar Event Processor 1605 または QRadar Event Processor 1628 を追加する必要があります。
- 別の国または州でイベントを収集および保管する場合は、データ収集に関する現地の法律に準拠するために、イベント・プロセッサーの追加が必要になることがあります。

データ・ノード

新しい QRadar デプロイメント環境や既存の QRadar デプロイメント環境でデータ・ノードを使用すると、必要に応じてオンデマンドでストレージや処理容量を追加することができます。データ・ノードを使用すると、より多くのデータを圧縮されていない状態で保存できるため、デプロイメントでの検索速度が向上します。

各コンポーネントについて詳しくは、「管理ガイド」を参照してください。

QRadar アプライアンスのサイズ見積もり

デプロイメントでどのような場合に特定の QRadar アプライアンスを使用するかについて以下の表で説明します。

表 3. QRadar アプライアンスの概要

アプライアンス	説明
QRadar 2100	従業員が 10 人から 200 人のデプロイメント向けの拡張不可のソリューション
QRadar 3105 (All-in-One)	QRadar 2100 よりも強化された能力を提供し、イベント・プロセッサーおよびフロー・プロセッサーを追加する機能を提供します。
QRadar 3105 (コンソール)	デプロイメントが 5000 イベント/秒 (EPS) を超える処理を行う場合は、QRadar 3105 (コンソール) を分散イベント・プロセッサーとともに使用する必要があります。QRadar 3105 (コンソール) は、オフボード・イベント処理およびストレージを使用して、リソースを解放します。これにより、レポートや検索結果のサービスを提供し、UI アクションの速度を向上させます。

表 3. *QRadar* アプライアンスの概要 (続き)

アプライアンス	説明
QRadar 3128 (All-in-One)	QRadar 3105 (All-in-One) よりも強化された能力を提供します。
QRadar 3128 (コンソール)	QRadar 3105 (コンソール) よりも強化された能力を提供します。
xx05 コレクターおよびプロセッサー	12 個のプロセッサー 64 GB の RAM 6.2 TB の使用可能ストレージ
xx28 コレクターおよびプロセッサー	28 個のプロセッサー 128 GB の RAM 40 TB の使用可能ストレージ パフォーマンスを向上させるには、xx28 コレクターおよびプロセッサーを QRadar 3128 (コンソール) とペアにして使用します。

フロー・プロセッサーを追加する場合

- NetFlow 収集速度が 31xx アプライアンスのフロー・レーティングを超える場合は、専用フロー・プロセッサーに移行する必要があります。
- デプロイメントに QRadar QFlow コレクターを追加する場合は、QFlow データを保管および処理するためにフロー・プロセッサーを追加する必要があります。
- 別の国または州でフローを収集および保管する場合は、データ収集に関する現地の法律に準拠するために、フロー・プロセッサーの追加が必要になることがあります。

関連概念:

63 ページの『第 11 章 問題のトラブルシューティング』
トラブルシューティングとは、問題を解決するための体系的な方法です。トラブルシューティングの目的は、想定どおりに機能しない理由とその問題の解決方法を判別することです。

53 ページの『第 9 章 データ・ノードの概要』
ここでは、IBM Security QRadar のデプロイメント環境内でデータ・ノードを使用する方法について説明します。

QRadar のインストールに関するハードウェア・アクセサリーおよびデスクトップ・ソフトウェアの前提条件

IBM Security QRadar 製品をインストールする前に、必要なハードウェア・アクセサリーとデスクトップ・ソフトウェアにアクセスできることを確認してください。

ハードウェア・アクセサリー

以下のハードウェア・コンポーネントにアクセスできることを確認してください。

- モニターおよびキーボード、またはシリアル・コンソール
- データを保管するすべてのシステム (QRadar コンソール、イベント・プロセッサー (Event Processor)・コンポーネントまたはQRadar QFlow コレクター・コンポーネントなど) のための無停電電源装置 (UPS)。
- ヌル・モデム・ケーブル (システムをシリアル・コンソールに接続する場合)。

重要: QRadar 製品では、ハードウェア・ベースの RAID (Redundant Arrays of Independent Disks) 実装がサポートされていますが、ソフトウェア・ベースの RAID インストールはサポートされていません。

デスクトップ・ソフトウェア要件

QRadar 製品ユーザー・インターフェースにアクセスするために使用するすべてのデスクトップ・システムに、Java™ ランタイム環境 (JRE) バージョン 1.7 または IBM 64-bit Runtime Environment for Java V7.0 がインストールされていることを確認してください。

関連タスク:

19 ページの『第 3 章 QRadar コンソールまたは管理対象ホストのインストール』
QRadar アプライアンスまたはユーザーのアプライアンスに、IBM Security QRadar コンソールまたは管理対象ホストをインストールします。

25 ページの『ユーザーのアプライアンスへの RHEL のインストール』
IBM Security QRadar で使用する Red Hat Enterprise Linux オペレーティング・システムをユーザーのアプライアンスにインストールできます。

33 ページの『仮想マシンでの QRadar ソフトウェアのインストール』
仮想マシンを作成したら、IBM Security QRadar ソフトウェアを仮想マシンにインストールする必要があります。

ファームウェア更新

QRadar アプライアンスの内部ハードウェア・コンポーネントについての追加機能と更新を活用するために、IBM Security QRadar アプライアンスのファームウェアを更新します。

ファームウェアの更新方法について詳しくは、Firmware update for QRadar (http://www-01.ibm.com/support/docview.wss?uid=swg27047121) を参照してください。

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 4. *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
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

Internet Explorer でのドキュメント・モードおよびブラウザー・モードの有効化

Microsoft Internet Explorer を使用して IBM Security QRadar 製品にアクセスする場合は、ドキュメント・モードおよびブラウザー・モードを有効にする必要があります。

手順

1. Internet Explorer Web ブラウザーで、F12 を押して「開発者ツール」ウィンドウを開きます。
2. 「ブラウザー モード」をクリックし、ご使用の Web ブラウザーのバージョンを選択します。
3. 「ドキュメント モード」をクリックし、ご使用の Internet Explorer リリースの「**Internet Explorer** 標準 **(Internet Explorer standards)**」を選択します。

関連概念:

6 ページの『QRadar のインストールに関するハードウェア・アクセサリーおよびデスクトップ・ソフトウェアの前提条件』
IBM Security QRadar 製品をインストールする前に、必要なハードウェア・アクセサリーとデスクトップ・ソフトウェアにアクセスできることを確認してください。

USB フラッシュ・ドライブのインストール

IBM Security QRadar ソフトウェアは、USB フラッシュ・ドライブを使用してインストールできます。

USB フラッシュ・ドライブによるインストールは、製品のフル・インストールになります。USB フラッシュ・ドライブを使用して、アップグレードや製品パッチの適用を行うことはできません。フィックスパックの適用については、フィックスパックのリリース・ノートを参照してください。

サポート対象のバージョン

以下のアプライアンスやオペレーティング・システムを使用して、ブート可能な USB フラッシュ・ドライブを作成できます。

- QRadar v7.2.1 以降のアプライアンス
- Red Hat Enterprise Linux 6.7 とともにインストールされた Linux システム
- Microsoft Windows Vista
- Microsoft Windows 7
- Microsoft Windows 2008
- Microsoft Windows 2008R2

インストールの概要

QRadar ソフトウェアを USB フラッシュ・ドライブからインストールするには、以下の手順を実行します。

1. ブート可能な USB フラッシュ・ドライブを作成します。
2. QRadar アプライアンスのソフトウェアをインストールします。
3. 製品保守リリースやフィックスパックがあれば、インストールします。

   フィックスパックおよび保守リリースのインストール手順については、リリース・ノートを参照してください。

QRadar アプライアンスを使用したブート可能な USB フラッシュ・ドライブの作成

IBM Security QRadar V7.2.1 以降のアプライアンスを使用して、QRadar ソフトウェアのインストールに使用できるブート可能な USB フラッシュ・ドライブを作成することができます。

始める前に

ブート可能な USB フラッシュ・ドライブを QRadar アプライアンスから作成するには、以下のアイテムにアクセスできる必要があります。

- 2 GB の USB フラッシュ・ドライブ
- QRadar V7.2.1 以降の ISO イメージ・ファイル
- 物理 QRadar アプライアンス

QRadar アプライアンスがインターネットに接続されていない場合は、インターネットにアクセスして、QRadar ISO イメージ・ファイルをデスクトップ・コンピューターまたは別の QRadar アプライアンスにダウンロードすることができます。次に、ISO ファイルを、ソフトウェアをインストールする QRadar アプライアンスにコピーします。

ブート可能な USB フラッシュ・ドライブを作成する際、フラッシュ・ドライブの内容は削除されます。

手順

1. QRadar ISO イメージ・ファイルをダウンロードします。
   a. IBM サポート Web サイト (www.ibm.com/support) にアクセスします。
   b. QRadar アプライアンスのバージョンに一致する IBM Security QRadar ISO ファイルを見つけます。
   c. ISO イメージ・ファイルを QRadar アプライアンス上の /tmp ディレクトリーにコピーします。
2. SSH を使用して、root ユーザーとして QRadar システムにログインします。
3. USB フラッシュ・ドライブを QRadar システムの USB ポートに挿入します。

   システムが USB フラッシュ・ドライブを認識するまでに、最大 30 秒かかる可能性があります。
4. 以下のコマンドを入力して、ISO イメージをマウントします。

   ```
   mount -o loop /tmp/<name of the ISO image>.iso /media/cdrom
   ```
5. 以下のコマンドを入力して、マウントされている ISO から /tmp ディレクトリーに USB 作成スクリプトをコピーします。

   ```
   cp /media/cdrom/post/create-usb-key.py /tmp/
   ```
6. 以下のコマンドを入力して、USB 作成スクリプトを開始します。

   ```
   /tmp/create-usb-key.py
   ```
7. Enter キーを押します。
8. 1 を押して、 ISO ファイルのパスを入力します。 以下に例を示します。

   ```
   /tmp/<name of the iso image>.iso
   ```
9. 2 を押して、USB フラッシュ・ドライブが含まれているドライブを選択します。
10. 3 を押して、USB キーを作成します。

    ISO イメージを USB フラッシュ・ドライブに書き込むプロセスは、完了するのに数分かかります。ISO が USB フラッシュ・ドライブにロードされると、確認メッセージが表示されます。
11. q を押して、USB キー・スクリプトを終了します。
12. QRadar システムから USB フラッシュ・ドライブを取り外します。
13. スペースを解放するために、/tmp ファイル・システムから ISO イメージ・ファイルを削除します。

次のタスク

アプライアンスへの接続がシリアル接続である場合は、シリアル接続専用アプライアンス用の USB フラッシュ・ドライブの構成を参照してください。

アプライアンスへの接続がキーボードおよびマウス (VGA) である場合は、USB フラッシュ・ドライブを使用した QRadar のインストールを参照してください。

Microsoft Windows を使用したブート可能な USB フラッシュ・ドライブの作成

Microsoft Windows のデスクトップ・システムまたはノートブック・システムを使用して、QRadar ソフトウェアのインストールに使用できるブート可能な USB フラッシュ・ドライブを作成することができます。

始める前に

ブート可能な USB フラッシュ・ドライブを Microsoft Windows システムを使用して作成するには、以下のアイテムにアクセスできる必要があります。

- 2 GB の USB フラッシュ・ドライブ
- 以下のいずれかのオペレーティング・システムでのデスクトップ・システムまたはノートブック・システム
  - Windows 7
  - Windows Vista
  - Windows 2008
  - Windows 2008R2

以下のファイルを、IBM Support Web サイト (www.ibm.com/support) からダウンロードする必要があります。

- QRadar V7.2.1 以降の Red Hat 64 ビット ISO イメージ・ファイル
- Create-USB-Install-Key (CUIK) ツール

以下のファイルをインターネットからダウンロードする必要があります。

- PeaZip Portable 4.8.1
- SYSLINUX 4.06

ヒント: ダウンロード・ファイルを見つけるには、Web で `Peazip Portal v4.8.1` および `Syslinux` を検索してください。

ブート可能な USB フラッシュ・ドライブを作成する際、フラッシュ・ドライブの内容は削除されます。

手順

1. Create-USB-Install-Key (CUIK) ツールを抽出して `c:¥cuik` ディレクトリーに入れます。
2. PeaZip Portable 4.8.1 および SYSLINUX 4.06 の `.zip` ファイルを `cuik¥deps` フォルダーにコピーします。

   例えば、`c:¥cuik¥deps¥peazip_portable-4.8.1.WINDOWS.zip` および `c:¥cuik¥deps¥syslinux-4.06.zip` です。

   `.zip` ファイルを解凍する必要はありません。これらのファイルは、`cuik/deps` ディレクトリーでのみ使用可能である必要があります。
3. USB フラッシュ・ドライブをコンピューターの USB ポートに挿入します。
4. USB フラッシュ・ドライブがドライブ名でリストされていることと、Microsoft Windows でアクセス可能であることを確認してください。

5. c:¥cuik¥cuik.exe を右クリックして、「管理者として実行」を選択し、**Enter** キーを押します。
6. 1 を押して、QRadar ISO ファイルを選択し、「開く」をクリックします。
7. 2 を押して、USB フラッシュ・ドライブに割り当てられたドライブ名に対応する番号を選択します。
8. 3 を押して、USB フラッシュ・ドライブを作成します。
9. **Enter** キーを押して、USB フラッシュ・ドライブの内容が削除されることを認識していることを確認します。
10. create と入力して、ブート可能な USB フラッシュ・ドライブを ISO イメージから作成します。 このプロセスには数分かかります。
11. **Enter** キーを押してから、q と入力して、Create_USB_Install_Key ツールを終了します。
12. USB フラッシュ・ドライブを、コンピューターから慎重に取り外します。

次のタスク

アプライアンスへの接続がシリアル接続である場合は、シリアル接続専用アプライアンス用の USB フラッシュ・ドライブの構成を参照してください。

アプライアンスへの接続がキーボードおよびマウス (VGA) である場合は、USB フラッシュ・ドライブを使用した QRadar のインストールを参照してください。

Red Hat Linux を使用したブート可能な USB フラッシュ・ドライブの作成

Red Hat v6.7 の Linux デスクトップ・システムまたはノートブック・システムを使用して、IBM Security QRadar ソフトウェアのインストールに使用できるブート可能な USB フラッシュ・ドライブを作成することができます。

始める前に

ブート可能な USB フラッシュ・ドライブを Linux システムで作成するには、以下のアイテムにアクセスできる必要があります。

- 2 GB の USB フラッシュ・ドライブ
- QRadar V7.2.1 以降の ISO イメージ・ファイル
- 以下のソフトウェアがインストール済みの Linux システム
  - Red Hat 6.7
  - Python 6.2 以降

ブート可能な USB フラッシュ・ドライブを作成する際、フラッシュ・ドライブの内容は削除されます。

手順

1. QRadar ISO イメージ・ファイルをダウンロードします。
   a. IBM サポート Web サイト (www.ibm.com/support) にアクセスします。
   b. IBM Security QRadar ISO ファイルを見つけます。

c. ISO イメージ・ファイルを QRadar アプライアンス上の /tmp ディレクトリーにコピーします。

2. 以下のパッケージが含まれるように Linux ベースのシステムを更新します。
   - syslinux
   - mtools
   - dosfstools
   - parted

   ご使用の Linux システムに固有のパッケージ・マネージャーについては、ベンダーの資料を参照してください。
3. root ユーザーとして QRadar システムにログインします。
4. USB フラッシュ・ドライブをシステムの前面の USB ポートに挿入します。

   システムが USB フラッシュ・ドライブを認識するまでに、最大 30 秒かかる可能性があります。
5. 以下のコマンドを入力して、ISO イメージをマウントします。

   ```
   mount -o loop /tmp/<name of the ISO image>.iso /media/cdrom
   ```
6. 以下のコマンドを入力して、マウントされている ISO から /tmp ディレクトリーに USB 作成スクリプトをコピーします。

   ```
   cp /media/cdrom/post/create-usb-key.py /tmp/
   ```
7. 以下のコマンドを入力して、USB 作成スクリプトを開始します。

   ```
   /tmp/create-usb-key.py
   ```
8. Enter キーを押します。
9. 1 を押して、ISO ファイルのパスを入力します。 以下に例を示します。

   ```
   /tmp/Rhe664QRadar7_2_4_<build>.iso
   ```
10. 2 を押して、USB フラッシュ・ドライブが含まれているドライブを選択します。
11. 3 を押して、USB キーを作成します。

    ISO イメージを USB フラッシュ・ドライブに書き込むプロセスは、完了するのに数分かかります。ISO が USB フラッシュ・ドライブにロードされると、確認メッセージが表示されます。
12. q を押して、USB キー・スクリプトを終了します。
13. システムから USB フラッシュ・ドライブを取り外します。

次のタスク

アプライアンスへの接続がシリアル接続である場合は、シリアル接続専用アプライアンス用の USB フラッシュ・ドライブの構成を参照してください。

アプライアンスへの接続がキーボードおよびマウス (VGA) である場合は、USB フラッシュ・ドライブを使用した QRadar のインストールを参照してください。

シリアル接続専用アプライアンス用の USB フラッシュ・ドライブの構成

ブート可能な USB フラッシュ・ドライブを使用して QRadar ソフトウェアをシリアル専用アプライアンスにインストールする前に、追加の構成ステップを実行しておく必要があります。

このタスクについて

アプライアンスに接続されているキーボードやマウスがある場合、この手順は必要ありません。

手順

1. ブート可能な USB フラッシュ・ドライブをアプライアンスの USB ポートに挿入します。
2. USB フラッシュ・ドライブ上で、`syslinux.cfg` ファイルを見つけます。
3. syslinux 構成ファイルを編集して、デフォルト・インストールを `default linux` から `default serial` に変更します。
4. syslinux 構成ファイルに対する変更内容を保存します。

次のタスク

これで、USB フラッシュ・ドライブを使用して QRadar をインストールする準備ができました。

USB フラッシュ・ドライブを使用した QRadar のインストール

ブート可能な USB フラッシュ・ドライブから QRadar をインストールするには、以下の手順を実行してください。

始める前に

ブート可能な USB フラッシュ・ドライブを使用して QRadar ソフトウェアをインストールするには、ブート可能な USB フラッシュ・ドライブを事前に作成しておく必要があります。

このタスクについて

以下の手順は、ブート可能な USB フラッシュ・ドライブを使用して QRadar ソフトウェアをインストールする方法についての一般的なガイダンスです。

完全なインストール・プロセスは、製品のインストール・ガイドに記載されています。

手順

1. 必要なハードウェアをすべてインストールします。
2. 次のオプションのいずれかを選択してください。
   - ノートブックをアプライアンスの背面のシリアル・ポートに接続します。
   - キーボードとモニターをそれぞれのポートに接続します。

3. ブート可能な USB フラッシュ・ドライブをアプライアンスの USB ポートに挿入します。
4. アプライアンスを再始動します。

   ほとんどのアプライアンスは、デフォルトで、USB フラッシュ・ドライブからブートできます。QRadar ソフトウェアを独自のハードウェアにインストールしている場合は、USB を優先させるようにデバイスのブート順序を設定することが必要な場合があります。

   アプライアンスの始動後、USB フラッシュ・ドライブはインストールのためにアプライアンスを準備します。このプロセスは、完了に最大 1 時間かかることがあります。
5. 「**Red Hat Enterprise Linux**」メニューが表示されたら、以下のいずれかのオプションを選択します。
   - キーボードおよびモニターを接続した場合は、「**VGA** コンソールを使用してインストールまたはアップグレード **(Install or upgrade using VGA console)**」を選択します。
   - シリアル接続を使用してノートブックを接続した場合は、「シリアル・コンソールを使用してインストールまたはアップグレード **(Install or upgrade using Serial console)**」を選択します。
6. SETUP と入力して、インストールを開始します。
7. ログイン・プロンプトが表示されたら、root と入力して、システムに root ユーザーとしてログインします。

   ユーザー名では大/小文字を区別します。
8. **Enter** キーを押し、プロンプトに従って QRadar をインストールします。

   完全なインストール・プロセスは、製品のインストール・ガイドに記載されています。

Third-party software on QRadar アプライアンス上のサード・パーティー・ソフトウェア

IBM Security QRadar は、Linux 上で構築されたセキュリティー・アプライアンスであり、攻撃に対抗する目的で設計されています。QRadar は、マルチユーザー汎用サーバーとして設計されたものではありません。この製品は、対象とする機能をサポートすることに特化して設計および開発されています。オペレーティング・システムおよびサービスは、安全な運用を目的として設計されています。QRadar は、組み込みファイアウォールを備え、暗号化された認証済みアクセスを要求するセキュア接続を通じてのみ管理アクセスを許可し、制御されたアップグレードと更新を提供します。QRadar では、従来型のアンチウィルス・エージェントまたはマルウェア・エージェントは不要であり、サポートされません。また、サード・パーティー・パッケージまたはサード・パーティー・プログラムのインストールもサポートされません。

第 2 章 管理対象ホストの帯域幅

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。

インストール後における管理対象ホストとコンポーネントのデプロイについて詳しくは、「*IBM Security QRadar SIEM* 管理ガイド」を参照してください。

第 3 章 QRadar コンソールまたは管理対象ホストのインストール

QRadar アプライアンスまたはユーザーのアプライアンスに、IBM Security QRadar コンソールまたは管理対象ホストをインストールします。

デプロイメントのすべての IBM Security QRadar アプライアンスのソフトウェア・バージョンのバージョンとフィックス・レベルが同一である必要があります。複数の異なるバージョンのソフトウェアを使用するデプロイメントはサポートされていません。

始める前に

以下の要件を満たしていることを確認してください。

- 必要なハードウェアがインストールされている。
- キーボードおよびモニターが VGA 接続を使用して接続されている。
- アクティベーション・キーが使用可能である。
- http://www.ibm.com/developerworks (http://www.ibm.com/developerworks/library/se-nic4qradar/) を参照する (統合ネットワーク・インターフェースを構成する場合)。

手順

1. `setup` と入力して続行し、root としてログインします。
2. 内部のプログラム使用条件に同意します。

   ヒント: ドキュメントを読み進むには、スペース・バー・キーを押します。
3. アクティベーション・キーを求めるプロンプトが出されたら、IBM から受け取った、4 つの部分に区切られた 24 桁の英数字ストリングを入力します。

   文字 I と数字の 1 は同じものとして扱われます。文字 O と数字の 0 (ゼロ) も同じものとして扱われます。
4. セットアップのタイプとして「標準 **(normal)**」、「Enterprise モデル (Enterprise model)」を選択し、時刻をセットアップします。
5. インターネット・プロトコルのバージョンを選択します。
   - IPv6 用に QRadar を自動構成する場合は、「はい」を選択します。
   - IPv4 または IPv6 用に QRadar の IP アドレスを手動で構成する場合は、「いいえ」を選択します。
6. 必要な場合は結合インターフェースのセットアップを選択します。
7. 管理インターフェースを選択します。
8. ウィザードの「ホスト名」フィールドに完全修飾ドメイン名を入力します。
9. 「**IP** アドレス」フィールドに静的 IP アドレスを入力するか、割り当てられている IP アドレスを使用します。

重要**:** このホストを高可用性 (HA) クラスター用のプライマリー・ホストとして構成し、自動構成で「はい」を選択した場合は、自動的に生成された IP アドレスをメモしておく必要があります。HA の構成時に、この IP アドレスを入力する必要があります。

詳しくは、「*IBM Security QRadar* 高可用性ガイド」を参照してください。

10. E メール・サーバーを使用しない場合は、「**E** メール・サーバー名」フィールドに `localhost` と入力します。
11. 「ルート・パスワード」フィールドで、以下の条件を満たすパスワードを入力します。
    - 5 文字以上使用されていること
    - スペースが含まれていないこと
    - 次の特殊文字は使用することができます: @、#、^、*。
12. 「終了」をクリックします。
13. インストール・ウィザードの指示に従って、インストールを完了します。

    このインストール・プロセスは、完了までに数分かかる場合があります。
14. ライセンス・キーを適用します。
    a. QRadar にログインします。

       `https://`*`IP_Address_QRadar`*

       デフォルトのユーザー名は `admin` です。パスワードは、root ユーザー・アカウントのパスワードです。
    b. 「**QRadar** にログイン」をクリックします。
    c. 「管理」タブをクリックします。
    d. 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。
    e. 「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。
    f. 「表示」リスト・ボックスから、「ライセンス」を選択して、ライセンス・キーをアップロードします。
    g. まだ割り振りられていないライセンスを選択し、「ライセンスへのシステムの割り振り」をクリックします。
    h. システムのリストからシステムを選択し、「ライセンスへのシステムの割り振り」クリックします。
15. 管理対象ホストを追加する場合は、「*IBM Security QRadar SIEM* 管理ガイド」を参照してください。

次のタスク

(https://apps.xforce.ibmcloud.com/) にアクセスし、インストール済み環境用のセキュリティー・アプリケーション をダウンロードします。詳しくは、「*IBM Security QRadar SIEM* 管理者ガイド」の『コンテンツ・マネジメント』の章を参照してください。

第 4 章 ユーザーのアプライアンスへの QRadar ソフトウェアのインストール

ユーザーのアプライアンスへ IBM Security QRadar を適切にインストールするには、Red Hat Enterprise Linux オペレーティング・システムをインストールする必要があります。

アプライアンスが QRadar デプロイメントのシステム要件を満たしていることを確認します。

重要: アプライアンスに QRadar および Red Hat Enterprise Linux 以外のソフトウェアをインストールしないでください。

QRadar ソフトウェアをユーザーのハードウェアにインストールする場合は、ここで QRadar ソフトウェア購入の一部として RHEL ライセンスを購入し、QRadar ソフトウェア ISO イメージに付属する RHEL を使用することができます。

QRadar の購入に RHEL オペレーティング・システムが含まれていない場合は、RHEL を別途インストールします。ご使用の QRadar システムに RHEL が含まれている場合は、パーティションの構成や他の RHEL の準備を行う必要はありません。 19 ページの『第 3 章 QRadar コンソールまたは管理対象ホストのインストール』に進んでください。

重要: IBM で承認されていない RPM パッケージをインストールしないでください。未承認の RPM インストールが QRadar ソフトウェアのアップグレード時の依存関係エラーの原因になったり、デプロイメントでのパフォーマンスの問題の原因になったりする場合もあります。YUM を使用してオペレーティング・システムを更新したり、未承認のソフトウェアを QRadar システムにインストールしたりしないでください。

ユーザーのアプライアンスへの QRadar のインストールの前提条件

ユーザーのアプライアンスに Red Hat Enterprise Linux (RHEL) オペレーティング・システムをインストールする前に、ご使用のシステムがシステム要件を満たしていることを確認します。

以下の表で、システム要件について説明します。

表 5. ユーザーのアプライアンスへの *RHEL* のインストールのシステム要件

要件	説明
サポートされるソフトウェアのバージョン	バージョン 6.7
ビット・バージョン	64 ビット
KickStart ディスク	サポートされていません

表 5. ユーザーのアプライアンスへの *RHEL* のインストールのシステム要件 (続き)

要件	説明
Network Time Protocol (NTP) パッケージ	オプション NTP をタイム・サーバーとして使用する場合は、NTP パッケージを必ずインストールしてください。
コンソール・システムのメモリー (RAM)	最小 32 GB **重要:** QRadar をインストールする前に、システム・メモリーをアップグレードする必要があります。
イベント・プロセッサー (Event Processor) のメモリー (RAM)	24 GB
QRadar QFlow コレクター のメモリー (RAM)	16 GB
コンソール・システムの空きディスク・スペース	最小 256 GB **重要:** 最適なパフォーマンスを得るため、最小ディスク・スペースの 2 倍から 3 倍の追加スペースが使用可能であることを確認してください。
QRadar QFlow コレクター・プライマリー・ドライブ	最小 70 GB
ファイアウォール構成	WWW (http、https) 有効 SSH 有効 **重要:** ファイアウォールを構成する前に、SELinux オプションを無効にしてください。QRadar インストール済み環境には、「システム・セットアップ」ウィンドウで更新可能なデフォルトのファイアウォール・テンプレートが含まれています。

注: EFI インストールはサポートされていません。

HA システムおよび XFS ファイル・システムでの QRadar ソフトウェア・インストールの準備

高可用性 (HA) の構成の一環として、QRadar インストーラーでは、ストレージ・ファイル・システム `/store/` に、複製プロセスのための最小容量のフリー・スペースを必要とします。XFS ファイル・システムは、フォーマット後にサイズを削減できないため、スペースを事前に割り振る必要があります。

HA システムで使用する XFS パーティションを準備するには、以下の作業を行う必要があります。

1. **`mkdir`** コマンドを使用して、以下のディレクトリーを作成します。
   - `/media/cdrom`
   - `/media/redhat`

2. 以下のコマンドを入力して、QRadar ソフトウェアの ISO イメージをマウントします。

   ```
   mount -o loop <path_to_QRadar_iso> /media/cdrom
   ```

3. 以下のコマンドを入力して、RedHat Enterprise Linux V6.7 ソフトウェアをマウントします。

   ```
   mount -o loop <path_to_RedHat_6.7_64bit_dvd_iso_1> /media/redhat
   ```

4. システムが HA ペアでプライマリー・ホストとして指定された場合は、以下のスクリプトを実行します。

   ```
   /media/cdrom/post/prepare_ha.sh
   ```

5. インストールを開始するには、以下のコマンドを入力します。

   ```
   /media/cdrom/setup
   ```

注: この手順は、HAセカンダリー・ホストでは必要ありません。

ユーザーのアプライアンスへの QRadar インストール済み環境に対する Linux オペレーティング・システムのパーティション・プロパティー

ユーザーのアプライアンスを使用する場合は、Red Hat Enterprise Linux オペレーティング・システムでデフォルトのパーティションを変更する代わりに、パーティションを削除してから再作成できます。

次の表に示す値を、Red Hat Enterprise Linux オペレーティング・システムでパーティションを再作成する際の参考として使用してください。

制約事項: 論理ボリューム・マネージャー (LVM) を使用した論理ボリュームのサイズ変更はサポートされていません。

表 *6. RHEL* のパーティションに関するガイド

パーティション	説明	マウント・ポイント	ファイル・システム・タイプ	サイズ **(Size)**	強制的にプライマリーにする	**SDA** または **SDB**
/boot	システム・ブート・ファイル	/boot	EXT4	200 MB	はい	SDA

表 6. *RHEL* のパーティションに関するガイド (続き)

パーティション	説明	マウント・ポイント	ファイル・システム・タイプ	サイズ **(Size)**	強制的にプライマリーにする	**SDA** または **SDB**
swap	RAM がいっぱいになるとメモリーとして使用される。	空	swap	4 GB から 8 GB の RAM を備えたシステム: スワップ・パーティションのサイズは RAM の容量と一致している必要があります。 8 GB から 24 GB の RAM を備えたシステム: スワップ・パーティションのサイズは RAM の 75% となるように構成します (最小値は 8 GB、最大値は 24 GB)。	いいえ	SDA
/	QRadar、オペレーティング・システム、および関連ファイルのインストール領域。	/	EXT4	20000 MB	いいえ	SDA
/store/tmp	QRadar 一時ファイルのストレージ域。	/store/tmp	EXT4	20000 MB	いいえ	SDA
/var/log	QRadar およびシステム・ログ・ファイルのストレージ域。	/var/log	EXT4	20000 MB	いいえ	SDA
/store	QRadar データおよび構成ファイルのストレージ域。	/store	XFS	[1]コンソール・アプライアンス: 使用可能なストレージの約 80%。 QFlow Collector およびストア・アンド・フォワード・イベント・コレクター以外の管理対象ホスト: 使用可能なストレージの約 90%。	いいえ	SDA ディスクが 2 つの場合は SDB

表 6. *RHEL* のパーティションに関するガイド (続き)

パーティション	説明	マウント・ポイント	ファイル・システム・タイプ	サイズ **(Size)**	強制的にプライマリーにする	**SDA** または **SDB**
/store/transient	ariel データベース・カーソルのストレージ域	/store/transient	XFS (コンソールの場合) EXT4 (管理対象ホストの場合)	[1]コンソール・アプライアンス: 使用可能なストレージの 20%。 QFlow Collector およびストア・アンド・フォワード・イベント・コレクター以外の管理対象ホスト: 使用可能なストレージの 10%。	いいえ	SDA ディスクが 2 つの場合は SDB
[1]/store および /store/transient の両方で、最初の 5 つのパーティションを作成した後の残りディスク・スペースの 100% を専有します。						

制限

以下のパーティションやそのサブパーティションを再フォーマットすると、今後のソフトウェア・アップグレードが失敗する可能性があります。

- /store
- /store/tmp
- /store/ariel
- /store/transient

ユーザーのアプライアンスへの RHEL のインストール

IBM Security QRadar で使用する Red Hat Enterprise Linux オペレーティング・システムをユーザーのアプライアンスにインストールできます。

このタスクについて

QRadar のインストール済み環境に RHEL オペレーティング・システムが含まれていない場合は、RHEL を別途インストールします。ご使用の QRadar システムに RHEL が含まれている場合は、 21 ページの『第 4 章 ユーザーのアプライアンスへの QRadar ソフトウェアのインストール』に進みます。

手順

1. Red Hat Enterprise Linux 6.7 オペレーティング・システム DVD ISO を、以下のいずれかのポータブル・ストレージ・デバイスにコピーします。
   - DVD (Digital Versatile Disk)
   - ブート可能な USB フラッシュ・ドライブ
2. アプライアンスにポータブル・ストレージ・デバイスを挿入し、アプライアンスを再始動します。
3. 開始メニューから次のいずれかのオプションを選択します。

- ブート・オプションとして USB または DVD ドライブを選択します。
- Extensible Firmware Interface (EFI) をサポートするシステムにインストールするには、システムを**レガシー**・モードで始動する必要があります。

4. プロンプトが出されたら、root ユーザーとしてシステムにログインします。
5. イーサネット・インターフェースのアドレス名指定に関する問題を防ぐため、「ようこそ (Welcome)」ページでタブ・キーを押し、Vmlinuz initrd=initrd.image 行の末尾に biosdevname=0 を追加します。
6. インストール・ウィザードの指示に従って、インストールを完了します。
   a. 「基本ストレージ・デバイス **(Basic Storage Devices)**」オプションを選択します。
   b. ホスト名を構成するときには、「ホスト名 **(Hostname)**」プロパティーに文字、数字、ハイフンを使用できます。
   c. ネットワークを構成するときには、「ネットワーク接続 (Network Connections)」ウィンドウで「システム **eth0 (System eth0)**」を選択し、「編集 **(Edit)**」をクリックして「自動的に接続する **(Connect automatically)**」を選択します。
   d. 「**IPv4** 設定 **(IPv4 Settings)**」タブの「方式 **(Method)**」リストから、「手動 **(Manual)**」を選択します。
   e. 「**DNS** サーバー **(DNS servers)**」フィールドに、コンマ区切りリストを入力します。
   f. 「カスタム・レイアウトの作成 **(Create Custom Layout)**」オプションを選択します。
   g. /、/boot、store/tmp、および /var/log の各パーティションのファイル・システム・タイプとして EXT4 を構成します。

      アプライアンスのタイプに基づくファイル・システム・タイプについて詳しくは、 23 ページの『ユーザーのアプライアンスへの QRadar インストール済み環境に対する Linux オペレーティング・システムのパーティション・プロパティー』を参照してください。
   h. ファイル・システム・タイプとしてスワップを使用して、スワップ・パーティションを再フォーマットします。
   i. 「基本サーバー **(Basic Server)**」を選択します。
7. インストールが完了したら、「リブート **(Reboot)**」をクリックします。

次のタスク

インストールの完了後、オンボード・ネットワーク・インターフェースの名前が eth0、eth1、eth2、および eth3 以外の場合は、ネットワーク・インターフェースの名前を変更する必要があります。

関連資料:

23 ページの『ユーザーのアプライアンスへの QRadar インストール済み環境に対する Linux オペレーティング・システムのパーティション・プロパティー』
ユーザーのアプライアンスを使用する場合は、Red Hat Enterprise Linux オペレーティング・システムでデフォルトのパーティションを変更する代わりに、パーティションを削除してから再作成できます。

第 5 章 QRadar SIEM および QRadar Log Manager の仮想アプライアンスのインストール

仮想アプライアンスに IBM Security QRadar SIEM と IBM Security QRadar Log Manager をインストールできます。サポートされており、最小システム要件を満たしている仮想アプライアンスを使用していることを確認してください。

制約事項: 論理ボリューム・マネージャー (LVM) を使用した論理ボリュームのサイズ変更、および EFI インストールはサポートされていません。

仮想アプライアンスをインストールするには、次のタスクを順に実行します。

- 仮想マシンを作成します。
- 仮想マシンに QRadar ソフトウェアをインストールします。
- 仮想アプライアンスをデプロイメントに追加します。

重要: 仮想マシンに QRadar および Red Hat Enterprise Linux 以外のソフトウェアをインストールしないでください。

サポートされる仮想アプライアンスの概要

仮想アプライアンスは、VMWare ESX 仮想マシンにインストールされている QRadar ソフトウェアで構成される IBM Security QRadar システムです。

仮想アプライアンスが仮想ネットワーク・インフラストラクチャーで提供する可視性および機能は、QRadar アプライアンスが物理環境で提供する可視性および機能と同一です。

仮想アプライアンスのインストール後に、デプロイメント・エディターを使用して仮想アプライアンスをデプロイメントに追加してください。アプライアンスの接続方法について詳しくは、「管理ガイド」を参照してください。

以下の仮想アプライアンスが使用可能です。

QRadar SIEM All-in-One Virtual 3199

この仮想アプライアンスは、ネットワークの振る舞いをプロファイルし、ネットワーク・セキュリティー上の脅威を特定できる QRadar SIEM システムです。
QRadar SIEM All-in-One Virtual 3199 仮想アプライアンスには、オンボードのイベント・コレクター (Event Collector)とイベント用の内部ストレージが組み込まれています。

QRadar SIEM All-in-One Virtual 3199 仮想アプライアンスは、以下の項目をサポートします。

- 最大 1,000 個のネットワーク・オブジェクト
- 間隔当たり 200,000 個のフロー (ライセンスに応じて異なります)
- 5,000 イベント/秒 (EPS) (ライセンスに応じて異なります)

- 750 個のイベント・フィード (ライセンスにデバイスを追加できます)
- NetFlow、sFlow、J-Flow、Packeteer、および Flowlog ファイルの外部フロー・データ・ソース
- QRadar QFlow コレクター およびレイヤー 7 のネットワーク・アクティビティー・モニター

QRadar SIEM All-in-One Virtual 3199 のキャパシティーを、ライセンス・ベースのアップグレード・オプションを超えて拡張するために、1 つ以上の QRadar SIEM Event Processor Virtual 1699 または QRadar SIEM Flow Processor Virtual 1799 仮想アプライアンスを追加できます。

QRadar SIEM Flow Processor Virtual 1799

この仮想アプライアンスは、QRadar SIEM 3105 または QRadar SIEM 3124 シリーズのアプライアンスと共にデプロイされます。この仮想アプライアンスは、ストレージを増加する目的で使用され、オンボードのイベント・プロセッサー (Event Processor)と内部ストレージが組み込まれています。

QRadar SIEM Flow Processor Virtual 1799 アプライアンスは、以下の項目をサポートします。

- 間隔当たり 600,000 個のフロー (トラフィック・タイプに応じて異なります)
- 2 TB 以上の専用フロー・ストレージ
- 1,000 個のネットワーク・オブジェクト
- QRadar QFlow コレクター およびレイヤー 7 のネットワーク・アクティビティー・モニター

ストレージを増加し、デプロイメントのパフォーマンスを向上させるために、QRadar SIEM Flow Processor Virtual 1799 アプライアンスを任意の QRadar SIEM 3105 シリーズまたは QRadar SIEM 3124 シリーズのアプライアンスに追加できます。

QRadar SIEM Event Processor Virtual 1699

この仮想アプライアンスは専用イベント・プロセッサー (Event Processor)です。これにより、高い EPS レートを管理するために QRadar SIEM デプロイメントを拡大できます。QRadar SIEM Event Processor Virtual 1699 にはオンボードのイベント・コレクター (Event Collector)、イベント・プロセッサー (Event Processor)、およびイベント用の内部ストレージが組み込まれています。

QRadar SIEM Event Processor Virtual 1699 アプライアンスは、以下の項目をサポートします。

- 最大 20,000 イベント/秒
- 2 TB 以上の専用イベント・ストレージ

QRadar SIEM Event Processor Virtual 1699 仮想アプライアンスは分散イベント・プロセッサー (Event Processor)・アプライアンスであり、QRadar SIEM 3105 またはQRadar SIEM 3124 シリーズのアプライアンスに接続する必要があります。

QRadar Data Node Virtual 1400

この仮想アプライアンスは、イベントとフローを保存および保管します。この仮想アプライアンスによりイベント・プロセッサーおよびフロー・プロセッサーの使用可能なデータ・ストレージが拡張され、また検索処理のパフォーマンスが向上します。

デプロイメントの EPS レートとデータ保存ルールに基づき、QRadar Data Node Virtual 1400 アプライアンス を適切にサイジングします。

データ保存ポリシーは、スタンドアロン・イベント・プロセッサーおよびフロー・プロセッサーに適用される場合と同様の方法で QRadar Data Node Virtual 1400 アプライアンスに適用されます。データ保存ポリシーはノードごとに評価されます。フリー・スペースなどの基準は、クラスター全体ではなく、個別の QRadar Data Node Virtual 1400 アプライアンスに基づいています。

データ・ノードは次のアプライアンスに追加できます。

- イベント・プロセッサー (16XX)
- フロー・プロセッサー (17XX)
- イベント/フロー・プロセッサー (18XX)
- オールインワン (2100 および 31XX)

QRadar Data Node Virtual 1400 アプライアンスに組み込まれているすべての機能を有効にするには、1400 のアクティベーション・キーを使用してインストールします。

QRadar VFlow Collector 1299

この仮想アプライアンスが仮想ネットワーク・インフラストラクチャーで提供する可視性と機能は、QRadar QFlow コレクター が物理環境で提供する可視性と機能と同一です。QRadar QFlow コレクター 仮想アプライアンスはネットワークの振る舞いを分析し、仮想インフラストラクチャー内でレイヤー 7 の可視性を提供します。ネットワークの可視性は、仮想スイッチへの直接接続から得られます。

QRadar VFlow Collector 1299 仮想アプライアンスは、最大で以下の項目をサポートします。

- 10,000 フロー/分
- 3 つの仮想スイッチと、管理インターフェースとして指定される 1 つのスイッチ。

QRadar VFlow Collector 1299 仮想アプライアンスは、NetFlow をサポートしていません。

仮想アプライアンスのシステム要件

IBM Security QRadar を確実に正しく機能させるには、使用する仮想アプライアンスがソフトウェアとハードウェアの最小要件を満たしていることを確認してください。

仮想アプライアンスをインストールする前に、以下の最小要件が満たされていることを確認してください。

表 7. 仮想アプライアンスの要件

要件	説明
VMware クライアント	VMWare ESX 5.0 VMWare ESX 5.1 VMWare ESX 5.5 VMWare クライアントについて詳しくは、VMware Web サイト (www.vmware.com) を参照してください。
QRadar VFlow コレクター、QRadar イベント・コレクター (Event Collector)、QRadar イベント・プロセッサー (Event Processor)、QRadar フロー・プロセッサー、QRadar オールインワン、および QRadar Log Manager の各アプライアンス上の仮想ディスク・サイズ	最小: 256 GB **重要:** 最適なパフォーマンスを得るため、最小ディスク・スペースの 2 倍から 3 倍の追加スペースが使用可能であることを確認してください。
QRadar QFlow コレクター アプライアンスの仮想ディスク・サイズ	最小: 70 GB
QRadar Risk Manager アプライアンスの仮想ディスク・サイズ	1 万件までの構成ソースの実装に推奨される仮想ディスク・サイズ: 1 TB
QRadar Vulnerability Manager プロセッサー・アプライアンスの仮想ディスク・サイズ	50000 個の IP アドレス - 500 GB 150000 個の IP アドレス - 750 GB 300000 個の IP アドレス - 1 TB
QRadar Vulnerability Manager スキャナー・アプライアンスの仮想ディスク・サイズ	20000 個の IP アドレス - 150 GB

仮想アプライアンスの最小メモリー所要量を以下の表に示します。

表 8. *QRadar* 仮想アプライアンスの最小メモリー所要量およびオプションのメモリー所要量

アプライアンス	最小メモリー所要量	推奨メモリー所要量
QRadar VFlow Collector 1299	6 GB	6 GB

表 *8. QRadar* 仮想アプライアンスの最小メモリー所要量およびオプションのメモリー所要量 *(*続き*)*

アプライアンス	最小メモリー所要量	推奨メモリー所要量
QRadar Event Collector Virtual 1599	12 GB	16 GB
QRadar SIEM Event Processor Virtual 1699	12 GB	48 GB
QRadar SIEM Flow Processor Virtual 1799	12 GB	48 GB
QRadar SIEM All-in-One Virtual 3199	24 GB	48 GB
QRadar Log Manager Virtual 8090	24 GB	48 GB
QRadar Risk Manager	24 GB	48 GB
QRadar Vulnerability Manager プロセッサー	8 GB	16 GB
QRadar Vulnerability Manager スキャナー	2 GB	4 GB

表 *9.* 「**CPU**」ページの設定例

プロセッサーの数	**QRadar** アプライアンスに基づくパフォーマンス
4	ログ・マネージャー 3190: 2500 イベント/秒以下。 ログ・マネージャー・イベント・プロセッサー 1690、または SIEM イベント・プロセッサー 1690: 2500 イベント/秒以下。 オールインワン 3190: 25000 フロー/分以下、500 イベント/秒以下。 フロー・プロセッサー 1790: 150,000 フロー/分。 専用コンソール 3190
8	ログ・マネージャー 3190: 5000 イベント/秒以下。 ログ・マネージャー・イベント・プロセッサー 1690、または SIEM イベント・プロセッサー 1690: 5000 イベント/秒以下。 オールインワン 3190: 50000 フロー/分以下、1000 イベント/秒以下。 フロー・プロセッサー 1790: 300,000 フロー/分。
12	オールインワン 3190: 100,000 フロー/分以下、1000 イベント/秒以下。
16	ログ・マネージャー・イベント・プロセッサー 1690、または SIEM イベント・プロセッサー 1690: 20,000 イベント/秒以下。 オールインワン 3190: 200,000 フロー/分以下、5000 イベント/秒以下。

関連タスク:

『仮想マシンの作成』
仮想アプライアンスをインストールするには、最初に VMWare ESX を使用して仮想マシンを作成する必要があります。

仮想マシンの作成

仮想アプライアンスをインストールするには、最初に VMWare ESX を使用して仮想マシンを作成する必要があります。

手順

1. VMware vSphere Client で「ファイル **(File)**」 > 「新規 **(New)**」 > 「仮想マシン **(Virtual Machine)**」をクリックします。
2. 「名前とロケーション **(Name and Location)**」を追加し、新しい仮想マシンの「データ・ストア」を選択します。
3. 以下のステップに従って、各項目の選択を行います。
   a. 「新規仮想マシンの作成 (Create New Virtual Machine)」ウィンドウの「構成 **(Configuration)**」ペインで、「カスタム **(Custom)**」を選択します。
   b. 「仮想マシンのバージョン **(Virtual Machine Version)**」ペインで「仮想マシンのバージョン**: 7 (Virtual Machine Version: 7)**」を選択します。
   c. 「オペレーティング・システム **(OS) (Operating System (OS))**」で「**Linux**」を選択してから「**Red Hat Enterprise Linux 6 (64-bit)**」を選択します。
   d. 「**CPU**」ページで、仮想マシンで必要とする仮想プロセッサーの数を構成します。CPU の設定について詳しくは、 29 ページの『仮想アプライアンスのシステム要件』を参照してください。
   e. 「メモリー・サイズ」フィールドで、デプロイメントに必要な RAM を入力または選択します。メモリー所要量について詳しくは、 29 ページの『仮想アプライアンスのシステム要件』を参照してください。
   f. 次の表を使用してネットワーク接続を構成します。

表 *10.* ネットワーク構成パラメーターの説明

パラメーター	説明
接続する **NIC** の数 **(How many NICs do you want to connect)**	少なくとも 1 つのネットワーク・インターフェース・コントローラー (NIC) を追加する必要があります。
アダプター **(Adapter)**	VMXNET3

   g. 「**SCSI** コントローラー **(SCSI controller)**」ペインで「**VMware Paravirtual**」を選択します。
   h. 「ディスク **(Disk)**」ペインで「新規仮想ディスクの作成 **(Create a new virtual disk)**」を選択し、次の表を使用して仮想ディスク・パラメーターを構成します。

表 11. 仮想ディスク・サイズとプロビジョニング・ポリシーのパラメーターの設定

プロパティー	オプション
容量	256 以上 (GB)
ディスクのプロビジョニング (Disk Provisioning)	シン・プロビジョン
拡張オプション (Advanced options)	構成しない

4. 「完了する準備ができています **(Ready to Complete)**」ページで設定を確認し、「終了 **(Finish)**」をクリックします。

次のタスク

仮想マシンに QRadar ソフトウェアをインストールします。

仮想マシンでの QRadar ソフトウェアのインストール

仮想マシンを作成したら、IBM Security QRadar ソフトウェアを仮想マシンにインストールする必要があります。

始める前に

アクティベーション・キーが使用できる状態であることを確認してください。

手順

1. VMware vSphere Client の左側のナビゲーション・ペインで、仮想マシンを選択します。
2. 右側のペインで「サマリー」タブをクリックします。
3. 「コマンド」ペインで「設定の編集 **(Edit Settings)**」をクリックします。
4. 「仮想マシンのプロパティー **(Virtual Machine Properties)**」ウィンドウの左側のペインで「**CD/DVD** ドライブ **1 (CD/DVD Drive 1)**」をクリックします。
5. 「装置タイプ」ペインで「データ・ストア **ISO** ファイル **(DataStore ISO File)**」を選択します。
6. 「デバイスの状況 **(Device Status)**」ペインで、「電源オン時に接続する **(Connect at power on)**」チェック・ボックスを選択します。
7. 「装置タイプ」ペインで「参照」をクリックします。
8. 「データ・ストアの参照 (Browse Datastores)」ウィンドウで QRadar 製品 ISO ファイルを見つけて選択し、「オープン」、「**OK**」の順にクリックします。
9. QRadar 製品 ISO イメージがインストールされたら、仮想マシンを右クリックして「電源 **(Power)**」 > 「電源オン **(Power On)**」をクリックします。
10. ユーザー名として `root` と入力して、仮想マシンにログインします。

    ユーザー名では大/小文字を区別します。
11. エンド・ユーザー使用許諾契約書 (EULA) が表示されることを確認します。

    ヒント: ドキュメントを読み進むには、スペース・バー・キーを押します。

12. アクティベーション・キーを求めるプロンプトが出されたら、IBM から受け取った、4 つの部分に区切られた 24 桁の英数字ストリングを入力します。

    文字 I と数字の 1 は同じものとして扱われます。文字 O と数字の 0 (ゼロ) も同じものとして扱われます。
13. セットアップのタイプとして「標準 **(normal)**」、「Enterprise モデル (Enterprise model)」を選択し、時刻をセットアップします。
14. インターネット・プロトコルのバージョンを選択します。
    - IPv6 用に QRadar を自動構成する場合は、「はい」を選択します。
    - IPv4 または IPv6 用に QRadar の IP アドレスを手動で構成する場合は、「いいえ」を選択します。
15. 必要な場合は結合インターフェースのセットアップを選択します。
16. 管理インターフェースを選択します。
17. ウィザードの「ホスト名」フィールドに完全修飾ドメイン名を入力します。
18. 「**IP** アドレス」フィールドに静的 IP アドレスを入力するか、割り当てられている IP アドレスを使用します。

    重要**:** このホストを高可用性 (HA) クラスター用のプライマリー・ホストとして構成し、自動構成で「はい」を選択した場合は、自動的に生成された IP アドレスをメモしておく必要があります。HA の構成時に、この IP アドレスを入力する必要があります。

    詳しくは、「*IBM Security QRadar* 高可用性ガイド」を参照してください。
19. E メール・サーバーを使用しない場合は、「**E** メール・サーバー名」フィールドに `localhost` と入力します。
20. 「ルート・パスワード」フィールドで、以下の条件を満たすパスワードを入力します。
    - 5 文字以上使用されていること
    - スペースが含まれていないこと
    - 次の特殊文字は使用することができます: @、#、^、*。
21. 「終了」をクリックします。
22. インストール・ウィザードの指示に従って、インストールを完了します。

    このインストール・プロセスは、完了までに数分かかる場合があります。
23. ライセンス・キーを適用します。
    a. QRadar にログインします。

       `https://IP_Address_QRadar`

       デフォルトのユーザー名は `admin` です。パスワードは、root ユーザー・アカウントのパスワードです。
    b. 「**QRadar** にログイン」をクリックします。
    c. 「管理」タブをクリックします。
    d. 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。
    e. 「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。

f. 「表示」リスト・ボックスから、「ライセンス」を選択して、ライセンス・キーをアップロードします。

g. まだ割り振りられていないライセンスを選択し、「ライセンスへのシステムの割り振り」をクリックします。

h. システムのリストからシステムを選択し、「ライセンスへのシステムの割り振り」クリックします。

次のタスク

(https://apps.xforce.ibmcloud.com/) にアクセスし、インストール済み環境用のセキュリティー・アプリケーション をダウンロードします。詳しくは、「*IBM Security QRadar SIEM* 管理者ガイド」の『コンテンツ・マネジメント』の章を参照してください。

関連タスク:

32 ページの『仮想マシンの作成』
仮想アプライアンスをインストールするには、最初に VMWare ESX を使用して仮想マシンを作成する必要があります。

デプロイメントへの仮想アプライアンスの追加

IBM Security QRadar ソフトウェアのインストール後に、仮想アプライアンスをデプロイメントに追加します。

手順

1. QRadar コンソールにログインします。
2. 「管理」タブで、「デプロイメント・エディター」アイコンをクリックします。
3. 「イベント・ビュー **(Event View)**」ページの「イベント・コンポーネント **(Event Component)**」ペインで、追加する仮想アプライアンス・コンポーネントを選択します。
4. 「新規コンポーネントの追加 **(Adding a New Component)**」タスク・アシスタントの最初のページで、仮想アプライアンスの固有の名前を入力します。

   仮想アプライアンスに割り当てる名前は、長さを 20 文字までとし、アンダースコアーやハイフンを含めることができます。
5. タスク・アシスタントのステップを実行します。
6. 「デプロイメント・エディター」メニューで、「ファイル」 > 「ステージングに保存 **(Save to staging)**」をクリックします。
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。
8. ライセンス・キーを適用します。
   a. QRadar にログインします。

      `https://IP_Address_QRadar`

      デフォルトのユーザー名は `admin` です。パスワードは、root ユーザー・アカウントのパスワードです。
   b. 「**QRadar** にログイン」をクリックします。
   c. 「管理」タブをクリックします。

d. 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。
e. 「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。
f. 「表示」リスト・ボックスから、「ライセンス」を選択して、ライセンス・キーをアップロードします。
g. まだ割り振りられていないライセンスを選択し、「ライセンスへのシステムの割り振り」をクリックします。
h. システムのリストからシステムを選択し、「ライセンスへのシステムの割り振り」クリックします。

関連タスク:

32 ページの『仮想マシンの作成』

仮想アプライアンスをインストールするには、最初に VMWare ESX を使用して仮想マシンを作成する必要があります。

第 6 章 リカバリー・パーティションからのインストール

IBM Security QRadar 製品をインストールすると、インストーラー (ISO イメージ) がリカバリー・パーティションにコピーされます。このパーティションから、QRadar 製品を再インストールできます。システムのデフォルト構成が復元されます。現行の構成とデータ・ファイルは上書きされます。

QRadar アプライアンスを再始動するときには、ソフトウェアを再インストールするオプションが表示されます。プロンプトに対して 5 秒以内に応答しない場合、システムは通常の方法による始動を続行します。構成とデータ・ファイルは保持されます。再インストール・オプションを選択すると、警告メッセージが表示されます。この場合は再インストールすることを確定する必要があります。

この警告メッセージは、アプライアンスにデータを保持できることを示しています。このデータにはイベントおよびフローが含まれます。保持オプションを選択すると、再インストールの前にデータがバックアップされ、インストールの完了後にデータがリストアされます。保持オプションを選択できない場合、データが存在するパーティションを使用できない可能性があるため、データをバックアップおよびリストアすることはできません。保持オプションがない場合、ハード・ディスク障害を示している可能性があります。保持オプションを選択できない場合は、お客様サポートにお問い合わせください。

重要: 保持オプションは、高可用性システムでは選択できません。高可用性アプライアンスのリカバリーについては、「*IBM Security QRadar High Availability Guide*」を参照してください。

QRadar バージョン 7.2.0 のソフトウェア・アップグレードを実行すると、既存の ISO ファイルが新しいバージョンに置き換えられます。

これらのガイドラインは、QRadar バージョン 7.2.0 の新規インストール、および QRadar バージョン 7.0 アプライアンス上の QRadar バージョン 7.0 の新規インストールからのアップグレードに適用されます。

リカバリー・パーティションからの再インストール

リカバリー・パーティションから IBM Security QRadar 製品を再インストールできます。

始める前に

アクティベーション・キーを見つけます。アクティベーション・キーは、IBM から受け取る、4 つの部分に区切られた 24 桁の英数字ストリングです。アクティベーション・キーは、以下のいずれかの場所にあります。

- ステッカーに印刷されてアプライアンス上に物理的に添付されています。
- 納品書に付属しています。すべてのアプライアンスがその関連するキーと共にリストされています。

アクティベーション・キーがない場合は、IBM サポート Web サイト (www.ibm.com/support) にアクセスしてアクティベーション・キーを入手してください。QRadar アプライアンスのシリアル番号を入力する必要があります。ソフトウェア・アクティベーション・キーの場合、シリアル番号は不要です。

デプロイメントにオフボード・ストレージ・ソリューションが含まれている場合は、QRadar を再インストールする前に、オフボード・ストレージを取り外す必要があります。再インストールが完了したら、外部ストレージ・ソリューションを再マウントできます。オフボード・ストレージの構成について詳しくは、「オフボード・ストレージ・ガイド」を参照してください。

手順

1. QRadar アプライアンスを再始動し、「出荷時状態で再インストール （**Factory re-install**）」を選択します。
2. `flatten` または `retain` と入力します。

   インストーラーにより、ハード・ディスクのパーティション化と再フォーマット、OS のインストールが実行され、その後 QRadar 製品が再インストールされます。フラット化または保存のプロセスが完了するまでお待ちください。このプロセスの完了までに数分かかることがあります。このプロセスが完了すると、確認が表示されます。
3. `SETUP` と入力します。
4. root ユーザーとしてログインします。
5. エンド・ユーザー使用許諾契約書 (EULA) が表示されることを確認します。

   ヒント: ドキュメントを読み進むには、スペース・バー・キーを押します。
6. QRadar コンソールをインストールする場合は、「エンタープライズ **(Enterprise)**」チューニング・テンプレートを選択します。
7. インストール・ウィザードの指示に従って、インストールを完了します。
8. ライセンス・キーを適用します。
   a. QRadar にログインします。

      `https://`*`IP_Address_QRadar`*

      デフォルトのユーザー名は `admin` です。パスワードは、root ユーザー・アカウントのパスワードです。
   b. 「**QRadar** にログイン」をクリックします。
   c. 「管理」タブをクリックします。
   d. 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。
   e. 「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。
   f. 「表示」リスト・ボックスから、「ライセンス」を選択して、ライセンス・キーをアップロードします。
   g. まだ割り振りられていないライセンスを選択し、「ライセンスへのシステムの割り振り」をクリックします。
   h. システムのリストからシステムを選択し、「ライセンスへのシステムの割り振り」クリックします。

第 7 章 QRadar のサイレント・インストールのセットアップ

IBM Security QRadar を「サイレントで」インストール、つまりインストールを無人で実行します。

始める前に

このインストールには、Red Hat Enterprise Linux オペレーティング・システムと、QRadar V7.2.6 ISO が必要です。バージョン番号と要件については、 21 ページの『第 4 章 ユーザーのアプライアンスへの QRadar ソフトウェアのインストール』を参照してください。

手順

1. QRadar をインストールするホストに RHEL をインストールして、必要なパーティションをセットアップします。詳しくは、 25 ページの『ユーザーのアプライアンスへの RHEL のインストール』を参照してください。
2. QRadar をインストールするホストに、root ユーザーとして SSH を使用してログオンします。
3. QRadar をインストールするホストでルート・ディレクトリーに移動し、以下の情報を含む AUTO_INSTALL_INSTRUCTIONS という名前のファイルを作成します。

   例: 以下の AUTO_INSTALL_INSTRUCTIONS ファイルの例は、America/Moncton タイム・ゾーンでの QRadar のサイレント・インストールの正しいパラメーターを示します。

   ```
   timezone=America/Moncton
   sectempl=Enterprise
   date=2015/05/19
   ntpserver=q1dc04.canlab.ibm.com
   ntpsync=1
   timechoice=manual
   nicid=eth0
   box_ip=1.2.3.4
   ip_v6=
   netmask=255.255.255.255
   ipverchoice=ipv4
   gateway_v6=
   hostname=name
   pdns=1.2.3.4
   bdns=5.6.7.8
   newkey=######-######-######-######
   defpass=password
   isconsole=yes
   setuptypechoice=normal
   is_ha_appl=0
   isconstandby=yes
   smtpname=localhost
   bonding_interfaces=
   bonding_options=
   bonding_enabled=false
   ```

   重要: AUTO_INSTALL_INSTRUCTIONS ファイルには拡張子は付けないでください。

サイレント・インストールの詳細:

表 12. サイレント・インストール・ファイルのパラメーター

パラメーター	必須かどうか	説明	許可される値
setuptypechoice	必須	このホストのインストール・タイプを指定します	normal- 標準 QRadar 管理対象ホストまたはコンソールのデプロイメント。 recovery - このホストでの高可用性 (HA) リカバリー・インストール。
timezone	必須	TZ データベースのタイム・ゾーン。詳しくは、http://timezonedb.com/を参照してください。	Europe/London America/Montreal America/New_York America/Los_Angeles Asia/Tokyo など
date	必須	このホストの現在の日付。 以下の形式を使用します。 YYYY/MM/DD 形式	
timechoice	必須	このホストが現在時刻を取得する方法を指定します	manual - time パラメーターに手動で入力する時刻。 server - ntpserver パラメーターで指定された Network Time Protocol (NTP) サーバーを使用します。
time	timechoice が manual に設定されている場合は必須。	24 時形式 (HH:MM:SS) の、ホストの時刻。	
ntpserver	timechoice が server に設定されている場合は必須。	Network Time Protocol (NTP) サーバーの FQHN または IP アドレス。	
ntpsync	timechoice が server に設定されている場合は必須。	NTP サーバーと同期する場合は 1、その他の場合は 0 を入力します。	

表 12. サイレント・インストール・ファイルのパラメーター (続き)

パラメーター	必須かどうか	説明	許可される値
nicid	必須	ネットワーク・インターフェース・カードの ID	値: eth0、eth1、ethx
management_iface	必須	管理インターフェースの ID	値: eth0、eth1、ethx
hostname	オプション	ご使用の QRadar システムの完全修飾ホスト名。	
ipverchoice	必須	このホストの IP 標準プロトコルを指定します。	IPv4、IPv6
box_ip	ipverchoice が IPv4 に設定されている場合は必須	ソフトウェアをインストールするホストの IP アドレス	有効な IPv4 アドレス
ip_v6	ipverchoice が IPv6 に設定されている場合は必須	必要に応じて QRadar インストールの IPv6 アドレスを入力します。	有効な IPv6 アドレス
netmask	ipverchoice が IPv4 に設定されている場合は必須	このホストのネットマスク	
gateway	ipverchoice が IPv4 に設定されている場合は必須	このホストのネットワーク・ゲートウェイ	有効な IPv4 アドレス
gateway_v6	ipverchoice が IPv6 に設定されている場合は必須	このホストのネットワーク・ゲートウェイ	有効な IPv6 アドレス
ip_v6_nocidr	オプション	クラスレス・ドメイン間ルーティング (CIDR) を使用しない IPv6 アドレス。	有効な IPv6 アドレス
pdns	ipverchoice が IPv4 に設定されている場合は必須	1 次 DNS サーバー。	有効な IPv4 アドレス
bdns	ipverchoice が IPv4 に設定されている場合は必須	2 次 DNS サーバー。	有効な IPv4 アドレス

表 12. サイレント・インストール・ファイルのパラメーター (続き)

パラメーター	必須かどうか	説明	許可される値
newkey	必須	QRadar インストールのアクティベーション・キー。	
defpass	必須	このホストに使用するデフォルトのルート・パスワード。	
isconsole	必須	このホストがデプロイメント内のコンソールかどうかを指定します	Y - このホストはデプロイメント内のコンソール N - このホストはコンソールではなく、別のタイプの管理対象ホスト (イベント・プロセッサー、フロー・プロセッサーなど)
sectempl	isconsole が Y に設定されている場合は必須	セキュリティー・テンプレート。	Enterprise - SIEM ベースのすべてのホストの場合 Logger - ログ・マネージャーの場合
is_ha_appl	必須	このホストが HA ペアかコンパニオン・ホストかを指定します。	0 - このホストは HA アプライアンス/インストールではない 1 - このホストは HA アプライアンス/インストールである
isconstandby	isconsole が Y に設定されている場合は必須。	このホストがスタンバイ HA コンソールかどうかを指定します	0 - このホストはスタンバイ HA コンソールではない 1 - このホストはスタンバイ HA コンソールである
clusterip	オプション	HA クラスターの IP アドレスを指定します。	ip_address
smtpname	必須	メール・サーバーまたは SMTP の名前 (localhost など) を入力します。	
bonding _interfaces	結合インターフェースを使用している場合は、必須です。	結合しているインターフェースのコンマ区切りの MAC アドレス。	mac_addresses

表 12. サイレント・インストール・ファイルのパラメーター (続き)

パラメーター	必須かどうか	説明	許可される値
bonding_options	結合インターフェースを使用している場合は、必須です。	結合インターフェース用の Linux オプション。	例: miimon=100 mode=4 lacp_rate=1
bonding enabled	結合インターフェースを使用している場合は、必須です。	結合インターフェースを使用中かどうか指定します。	true または false

4. WinSCP などのセキュア・ファイル転送プロトコル (SFTP) プログラムを使用して、QRadar をインストールするホストに QRadar ISO をコピーします。
5. WinSCP などのプログラムを使用して、QRadar をインストールするホストに RHEL ISO をコピーします。
6. 以下のコマンドを使用して /media/cdrom ディレクトリーを作成します。

   ```
   mkdir /media/cdrom
   ```

7. 以下のコマンドを使用して /media/redhat ディレクトリーを作成します。

   ```
   mkdir /media/redhat
   ```

8. 以下のコマンドを使用して QRadar ISO をマウントします。

   ```
   mount -o loop <qradar.iso> /media/cdrom
   ```

9. 以下のコマンドを使用して RHEL ISO をマウントします。

   ```
   mount -o loop <RHEL.iso> /media/redhat
   ```

10. 以下のコマンドを使用して QRadar セットアップを実行します。

    ```
    /media/cdrom/setup
    ```

第 8 章 クラウド環境での QRadar デプロイメントの概要

IBM Security QRadar ソフトウェアのインスタンスを、Amazon Web Services によってホストされているクラウド・サーバーにインストールすることができます。QRadar のオンプレミス・インスタンスとクラウド・インスタンスとの間にセキュアな通信を確立するには、VPN 接続を構成する必要があります。OpenVPN 接続を構成することも、別のメカニズム (クラウド・プロバイダーの VPN インフラストラクチャーなど) を使用することもできます。

重要: セキュリティー・データが危険にさらされることを避けるために、以下の要件が満たされていることを確認してください。

- 強力なルート・パスワードを設定します。
- ポート 443 (https)、22 (ssh)、10000 (webmin)、および 1194 (UDP、OpenVPN の場合は TCP) へは特定の接続のみを許可します。

以下の順序で、クラウドに QRadar を構成します。

1. QRadar を Amazon Web Services (AWS) にインストールします。
2. クラウドおよびオンプレミスのホストに以下のロールを定義します。
   - VPN トンネルのサーバー・エンドポイント。
   - VPN トンネルのクライアント・エンドポイント。
   - VPN トンネルへ向かうトラフィックを自身のローカル VPN エンドポイントを通して発送するメンバー・ホスト。
   - VPN トンネルの別サイドのホストと通信する必要がないホストの場合は指定なし。
3. QRadar ファイアウォール設定が、ご使用のネットワーク・セキュリティーを保護していることを確認します。

Amazon Web Services での QRadar ホストの構成

IBM Security QRadar のオンプレミス・インスタンスと Amazon Web Services (AWS) インスタンスとの間のセキュア接続を構成します。

始める前に

1. AWS で鍵ペアを構成します。
2. 以下の要件を満たす Amazon EC2 インスタンスを作成します。

表 *13. AWS* インスタンスの要件

要件	値
イメージ	RHEL-6.7_HVM_Beta_20150714-x86_64-1-Hourly-GP2
インスタンス・タイプ	m4.2xlarge
ストレージ	3 x 100 GB のボリューム

表 13. AWS インスタンスの要件 (続き)

要件	値
セキュリティー・グループ	リストにある IP アドレス。ポート 22 および 443 を開いておきます。

重要: 以下の手順内のコマンドはサンプルです。コマンドの値はデプロイメントによって異なります。

SSH を使用してインスタンスにログインするには AWS インスタンス・キーが必要です。

AWS が提供する RedHat Enterprise Linux (RHEL) v6.7 のロードでは、XFS は現在サポートされていません。ext4 を使用してください。

重要: AWS QRadar のインストール済み環境では、高可用性 (HA) はサポートされていません。

手順

1. 以下のコマンドを入力して、AWS インスタンスにログインします。インスタンスの構成時に作成した鍵ペアを使用します。

   ```
   ssh -i <your_key>.pem ec2-user@<public_IP_address>
   ```

2. 以下のコマンドを使用して、AWS インスタンスの root のシェルに切り替えます。

   ```
   sudo su -
   ```

3. 以下のようにして、構成するデバイスを決定します。
   a. lsblk コマンドを入力して、デバイスの詳細をリストします。
   b. パーティションがなく、必要なストレージがあるデバイスを見つけます。

   ```
   [root@ip-172-31-13-123 ~]# lsblk
   NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
   xvda
         202:0 0 100G 0 disk
   └─xvda1 202:1 0 100G 0 part /
   xvdc 202:32 0 100G 0 disk
   xvdb 202:16 0 100G 0 disk
   ```

   ブロック・デバイスを見つけたら、そのデバイス名とデバイス・データを環境変数としてエクスポートして、後続のステップで使用できるようにします。前の例の場合、次のコマンドを入力します。

   ```
   export device_name=/dev/xvdc
   ```

   ```
   export device_data=/dev/xvdb
   ```

4. ディスクのパーティション・タイプ (ラベル) を作成するために、次のコマンドを入力します。

   ```
   parted -a optimal --script ${device_name} -- mklabel gpt
   ```

   ```
   parted -a optimal --script ${device_data} -- mklabel gpt
   ```

5. デバイスにこれらのパーティションを作成するには、以下のコマンドを入力します。

注: 以下の割り振りはサンプルです。パーティションについて詳しくは、「*IBM Security QRadar* インストール・ガイド」を参照してください。

```
parted -a optimal --script $device_name -- mkpart swap 0% 30%
parted -a optimal --script ${device_name} -- mkpart ext4 30% 60%
parted -a optimal --script ${device_name} -- mkpart ext4 60% 100%
parted -a optimal --script ${device_data} -- mkpart ext4 0% 80%
parted -a optimal --script ${device_data} -- mkpart ext4 80% 100%
```

6. パーティション化されたデバイスに以下のファイル・システムを作成するには、以下のコマンドを入力します。

```
mkswap -L swap1 ${device_name}1
mkfs.ext4 ${device_name}2
mkfs.ext4 ${device_name}3
mkfs.ext4 ${device_data}1
mkfs.ext4 ${device_data}2
```

7. 以下の名前を使用してパーティションにラベルを付けます。

```
e2label ${device_name}2 /var/log
e2label ${device_name}3 /store/tmp
e2label ${device_data}2 /store/transient
e2label ${device_data}1 /store
```

8. /etc/fstab ファイルに /dev/<*device_name*> /mnt または /dev/<*device_data*> /mnt という行がある場合は、これらの行をコメント化します。

9. 以下のコマンドを入力して、必要な項目を /etc/fstab ファイルに追加します。

```
eval `blkid -t LABEL=/store -o export` ; echo UUID=$UUID $LABEL $TYPE
 defaults,noatime 1 1 >> /etc/fstab
eval `blkid -t LABEL=/store/transient -o export` ; echo
      UUID=$UUID /store/transient $TYPE defaults,noatime 1 1 >> /etc/fstab
eval `blkid -t LABEL=/var/log -o export` ; echo UUID=$UUID $LABEL $TYPE
 defaults,noatime 1 1 >> /etc/fstab
echo  "${device_name}1
 swap  swap defaults 0 0" >> /etc/fstab
```

10. 以下のコマンドを入力して、/store ディレクトリーを作成してマウントします。

```
mkdir /store
mount /store
mkdir /store/tmp
mount /store/tmp
mkdir /store/transient
mount /store/transient
cd /var; mv log oldlog; mkdir log; mount /var/log; mv oldlog/* log
```

11. デバイス間のスワップを有効にするには、以下のコマンドを入力します。

```
swapon -a
```

12. /etc/sysconfig/i18n の行に、以下のストリング (引用符を含む) が含まれていることを確認します。

```
LANG="en_US.UTF-8"
```

13. デバイスに ISO イメージをコピーするには、以下のコマンドを入力します。

```
scp -i key.pem qradar.iso ec2-user@<Public_DNS>:qradar.iso
```

ここで、

- *qradar.iso* は、QRadar のインストール ISO イメージの名前です。
- *key.pem* は、ボックスにログインするためのキーです。

- *Public_DNS* はホストのドメイン名です。

14. ISO イメージをマウントするには、以下のコマンドを入力します。

```
mkdir /media/cdrom
mount -o loop /home/ec2-user/qradar.iso /media/cdrom
```

15. 次のコマンドを使用して不足している依存関係を構成します。

```
yum  install -y libxml2 libxml2.i686 audit-libs audit-libs.i686 glibc
glibc.i686 device-mapper-multipath zlib zlib.i686 libcom_err
libcom_err.i686 nspr nspr.i686 nss nss.i686 nss-util nss-util.i686
krb5-libs krb5-libs.i686 keyutils-libs keyutils-libs.i686
openssl   openssl.i686 httpd-tools httpd-devel httpd mod_ssl keyutils
keyutils.i686 keyutils-libs keyutils-libs.i686 openldap openldap.i686
openldap-clients cyrus-sasl-lib cyrus-sasl-lib.i686 pam pam.i686 libgcc
libgcc.i686 elfutils-libelf  elfutils-libelf.i686
libstdc++   libstdc++.i686
```

```
yum remove php.x86_64 php-cli.x86_64 php-common.x86_64
php-devel.x86_64 php-imap.x86_64 samba-common samba-winbind-clients
samba-client samba-winbind
httpd httpd-tools mod_ssl
```

```
sed -i -e's/plugins=1/plugins=0/' /etc/yum.conf
```

16. セットアップ・プログラムを開始するには、以下のコマンドを入力します。

```
/media/cdrom/setup
```

クラウドのインストール済み環境用のサーバー・エンドポイントの構成

IBM Security QRadar コンソールがオンプレミスであり、クラウド内に追加の処理ノードおよびストレージ・ノードがインストールされている場合は、OpenVPN を使用してクラウド・サーバーのサーバー・エンドポイントを構成します。

このタスクについて

サーバー・エンドポイントには以下の事項が必要です。

- OpenVPN のメイン構成ファイル。
- サーバー構成ファイル内での各クライアントに対するルーティング指示。
- 接続可能な各クライアントに対するルーティング指示を記録する、各クライアント用の構成ファイル。
- トンネル経由での転送を許可する追加の iptables ルール。
- カーネルで IP フォワードが有効になっていること。
- サーバーおよびクライアントを認証するのに使用される証明書を発行する、カスタム認証局 (CA)。
- ローカルの CA によって発行されたサーバー証明書。

OpenVPN ツールのオプションについて詳しくは、`-h` を入力してください。

手順

1. サーバー・エンドポイントを指定するには、以下のコマンドを入力してクラウド内のサーバー・エンドポイントを定義します。

```
/opt/qradar/bin/vpntool server server_host_IP_address network_address_behind_VPN
```

例:

```
/opt/qradar/bin/vpntool server 1.2.3.4 5.6.7.8/24
```

ネットワークがクライアントおよびサーバーで UDP モードではなく TCP モードを必要とする場合は、必要な IP アドレスを指定して以下のコマンドを入力します。

```
/opt/qradar/bin/vpntool server server_host_IP_address
 network_address_behind_VPN --tcp
```

サーバー・エンドポイントを定義すると、VPNtool サーバーによって以下のタスクが完了されます。

- ローカルの認証局が確立されていない場合は、CA が初期化され、CA のキーおよび証明書が作成されます。
- ローカルの CA が、このサーバー・エンドポイントが使用するキーおよび証明書を作成します。
- 構成プロパティーが、VPN 構成ファイルに書き込まれます。

2. 構成を作成してデプロイするには、以下のコマンドを入力します。

```
/opt/qradar/bin/vpntool deploy
```

構成を作成してデプロイすると、VPNtool サーバーが以下のタスクを実行します。

- OpenVPN サーバーの構成が生成され、/etc/openvpn ディレクトリーにコピーされます。
- CA 証明書、およびサーバー・キーと証明書が、/etc/openvpn/pki 内の標準の場所にコピーされます。
- IPtables ルールが構成され、再ロードされます。
- /etc/sysctl.conf ファイルを更新することにより、IP フォワードが有効になり、永続化されます。

3. サーバーを始動するには、以下のコマンドを入力します。

```
/opt/qradar/bin/enable --now
```

/opt/qradar/bin/enable --now を入力すると、永続的に有効な状態が作成され、システムの再開時に自動的に OpenVPN が開始されます。

クラウドのインストール済み環境用のクライアント・ネットワークの構成

オンプレミスの環境では、OpenVPN を使用してクラウド内のエンドポイントと通信するクライアント・ネットワークを構成します。

このタスクについて

クライアントには、以下の事項が必要です。

- OpenVPN のメイン構成ファイル。
- トンネル経由での転送を許可する追加の iptables ルール。
- カーネルで IP フォワードが有効になっていること。
- ローカルの CA によって発行されたクライアント証明書。

手順

1. サーバー上で以下のコマンドを入力して、サーバーに新規クライアントを通知します。

```
/opt/qradar/bin/vpntool addclient Console name, role,
 or IP  1.2.3.4/24
```

サーバーに対するクライアントの通知には、以下のタスクが含まれます。

- CA 証明書が既知の場所にコピーされます。
- PKCS#12 ファイルからクライアントのキーおよび証明書が抽出され、既知の場所にコピーされます。
- クライアントの構成プロパティーが VPN 構成ファイルに書き込まれます。

2. 以下のコマンドを使用して、サーバーのデプロイと再始動を行います。

```
/opt/qradar/bin/vpntool deploy
service openvpn restart
```

3. 生成されたクライアント資格情報ファイルと CA ファイルを、このクライアント・エンドポイント用に使用される QRadar ホストにコピーします。

例:

```
scp root@ server_IP_address :/opt/qradar/conf
/vpn/pki/ca.crt /root/ca.crtscp root@ server_IP_address
:/opt/qradar/conf/vpn/pki/Console.p12 /root/Console.p12
```

4. クライアントで、以下のようにしてホストを VPN クライアントとして構成します。

```
/opt/qradar/bin/vpntool client server_IP_address
ca.crt client.pk12
```

ネットワークの要件によりクライアントおよびサーバーで UDP モードを構成できない場合は、TCP を使用できます。

```
/opt/qradar/bin/vpntool client server_IP_address
/root/ca.crt /root/Console.p12 --tcp
```

5. 構成を作成してデプロイするには、以下のコマンドを入力します。

```
/opt/qradar/bin/vpntool deploy
```

以下のステップにより、構成が作成されてデプロイされます。

- クライアントの OpenVPN 構成ファイルが生成され、/etc/openvpn 内の場所にコピーされます。
- CA 証明書、およびクライアント・キーと証明書が、/etc/openvpn/pki 内の標準の場所にコピーされます。
- Iptables ルールが生成され、ロードされます。
- /etc/sysctl.conf ファイルを更新することにより、IP フォワードが有効になり、永続化されます。

6. クライアントを開始するには、以下のコマンドを入力します。

```
/opt/qradar/bin/enable --now
```

/opt/qradar/bin/enable --now を入力すると、永続的に有効な状態が作成され、システムの再開時に自動的に OpenVPN が開始されます。

7. HTTP プロキシー経由でクライアントを接続するには、以下のコマンドを入力します。

```
/opt/qradar/bin/vpntool client IP Address  /root/ca.crt
 /root/Console.p12 --http-proxy= IP Address:port
```

- このコマンドで TCP を入力しなくても、プロキシー構成は常に TCP モードになります。
- プロキシー認証の構成オプションについては、OpenVPN の資料を参照してください。それらの構成オプションを以下のファイルに追加してください。

  ```
  /etc/openvpn/client.conf
  ```

クラウドのインストール済み環境用のメンバーの構成

サーバーまたはクライアントではない IBM Security QRadar ホストに対するセキュア接続を確立するには、OpenVPN を使用します。

手順

以下のコマンドを使用して、QRadar SIEM ホストをローカル VPN に参加させ、このホストがトンネルの別サイドのホストと直接通信するようにします。

```
/opt/qradar/bin/vpntool join local_host_IP_address remote host IP address
/opt/qradar/bin/vpntool deploy
```

第 9 章 データ・ノードの概要

ここでは、IBM Security QRadar のデプロイメント環境内でデータ・ノードを使用する方法について説明します。

新しい QRadar デプロイメント環境や既存の QRadar デプロイメント環境でデータ・ノードを使用すると、必要に応じてオンデマンドでストレージや処理容量を追加することができます。

データ収集とは関係なく、ストレージや処理能力をスケーリングすることができます。その結果として、適切なストレージと処理能力を持つデプロイメント環境が構成されます。データ・ノードはプラグ・アンド・プレイです。いつでもデプロイメント環境に追加することができます。データ・ノードは、既存のデプロイメント環境にシームレスに統合されます。

デプロイメント環境内のデータ・ボリュームを増やすには、データの圧縮を迅速に行う必要があります。データの圧縮を行うと、システムのパフォーマンスが低下します。これは、分析を実行する前に、照会済みデータを解凍する必要があるためです。データ・ノード・アプライアンスをデプロイメント環境に追加すると、従来よりも長期間にわたって、データを解凍したままの状態にしておくことができます。

QRadar のデプロイメント環境では、イベント・プロセッサー、フロー・プロセッサー、付属のデータ・ノードにわたってすべての新規データが配布されます。

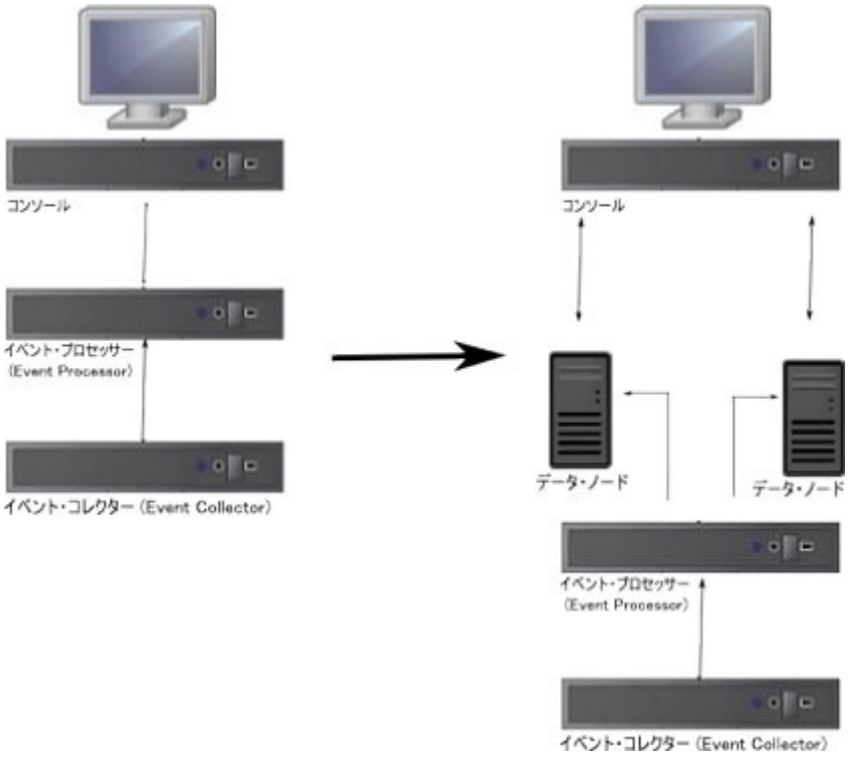

図 2. データ・ノード・アプライアンスを追加する前と追加した後の *QRadar* デプロイメント環境

クラスター化

データ・ノードはデプロイメント環境に容量を追加しますが、デプロイメント環境全体にデータを配布することにより、パフォーマンスも向上させます。クラスター全体のシステム・リソースを使用して、多くのホストで照会が実行されます。クラスター化を行うと、クラスター化されていない場合と比較して、検索速度が数倍も速くなります。

デプロイメント環境に関する考慮事項

- データ・ノードは、QRadar 7.2.2 以降で使用することができます。
- データ・ノードは、QRadar デプロイメント環境のイベント・プロセッサーやフロー・プロセッサーに類似した検索機能と分析機能を実行します。クラスター上での操作は、最も処理速度の遅いクラスター・メンバーの影響を受けます。データ・ノードのサイズをデプロイメント環境内のイベント・プロセッサーやフロー・プロセッサーと同程度のサイズにすると、データ・ノードのシステム・パフォーマンスが向上します。このサイズ調整を容易にするために、データ・ノードは XX05 コア・アプライアンスと XX28 コア・アプライアンスの両方で使用することができます。
- データ・ノードは、(ハードウェア上の) ソフトウェア、物理ノード、アプライアンスという 3 つの形式で使用することができます。1 つのクラスター内で、これらの形式を組み合わせて使用することができます。

帯域幅と待ち時間

クラスター内のホスト間に 1 Gbps のリンクを設定し、待ち時間が 10 ミリ秒未満になるようにしてください。

互換性

データ・ノードは、イベント・プロセッサー・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 (オールインワン・アプライアンスを含む) を持つすべての既存の QRadar アプライアンスに対応しています。データ・ノードは、QRadar Incident Forensics PCAP アプライアンスには対応していません。

データ・ノードは、高可用性 (HA) をサポートしています。

インストール

データ・ノードは標準の TCP/IP ネットワーキングを使用するため、専用の相互接続ハードウェアや特殊な相互接続ハードウェアは必要ありません。他の QRadar アプライアンスをインストールする際に、現在のデプロイメント環境に追加したいデータ・ノードを個別にインストールしてください。 QRadar デプロイメント・エディターを使用して、データ・ノードをイベント・プロセッサーまたはフロー・プロセッサーに関連付けてください。詳しくは、「*IBM Security QRadar* 管理ガイド」を参照してください。

多対 1 構成を使用して、1 つのイベント・プロセッサーまたはフロー・プロセッサーに複数のデータ・ノードを関連付けることができます。

データ・ノード・アプライアンスを使用して HA のペアをデプロイする場合は、HA のペアを同期化する前に、高可用性アプライアンスを使用して、データのインストール、デプロイ、再バランシングを行ってください。HA のデータの再バランス処理と複製処理を組み合わせると、パフォーマンスが大幅に低下します。データ・ノードの導入先となる既存のアプライアンス上に高可用性が構成されている場合は、クラスターの再バランス処理が完了したら、HA 接続を切断して再確立することをお勧めします。

使用中止

他の QRadar アプライアンスと同様に、デプロイメント・エディターを使用して、データ・ノードをデプロイメント環境から削除することができます。この方法でデータ・ノードの使用を中止しても、バランス化されたホスト上のデータが消去されることはありません。データを取得して、アーカイブや再配布を行うことができます。

データの再バランシング

データ・ノードをクラスターに追加すると、各データ・ノードにデータが均等に配布されます。それぞれのデータ・ノード・アプライアンスで、同じ割合の使用可能スペースが確保されます。クラスターに追加された新しいデータ・ノードにより、クラスターのイベント・プロセッサーとフロー・プロセッサーから追加の再バランス処理が開始され、新しく追加されたデータ・ノード・アプライアンス上に十分なディスク使用量が確保されます。

QRadar 7.2.3 以降、データの再バランス処理は、照会やデータ収集などの他のクラスター・アクティビティーと並行して自動的に実行されるようになりました。データの再バランス処理中にダウン時間は発生しません。

データの再バランス処理が完了するまで、データ・ノードによってクラスター内のパフォーマンスが向上することはありません。再バランス処理により、検索操作の実行中にパフォーマンスが多少低下することがありますが、データ収集やデータ処理が影響を受けることはありません。

管理と運用

データ・ノードは自己管理機能を持っているため、ユーザーが通常の保守操作を定期的に行う必要はありません。QRadar は、データ・ノード・アプライアンスを含むすべてのホストについて、データのバックアップなどのアクティビティー、高可用性、保存ポリシーを管理します。

障害

データ・ノードで障害が発生した場合は、残りのクラスター・メンバーがデータの処理を続行します。

障害が発生したデータ・ノードが復旧すると、クラスター内の適切なデータ配分を維持するためのデータ再バランシングが実行され、その後通常処理が再開されます。ダウン時間中は、障害が発生したデータ・ノードのデータは使用できなくなります。

アプライアンスの交換や QRadar の再インストールが必要になるような重大な障害が発生した場合は、デプロイメント環境でのデータ・ノードの使用を中止し、通常のインストール手順でそれらのデータ・ノードを置き換えてください。デプロイを行う前に、障害時に失われずに残ったデータを、すべて新しいデータ・ノードにコピーしてください。再バランス処理のアルゴリズムはデータ・ノード上に存在するデータを対象とし、障害中に収集されたデータのみをシャッフルします。

HA のペアとともにデプロイされたデータ・ノードの場合、ハードウェアで障害が発生するとフェイルオーバーが実行されるため、システムは引き続き正常に稼働します。

関連概念:

3 ページの『QRadar コンポーネント』

IBM Security QRadar は、ネットワーク上のデバイスやアプリケーションによって使用されるログ・ソースからのイベント・データを統合します。

第 10 章 ネットワーク設定の管理

IBM Security QRadar システムのネットワーク設定を変更するには、qchange_netsetup スクリプトを使用します。構成可能なネットワーク設定には、ホスト名、IP アドレス、ネットワーク・マスク、ゲートウェイ、DNS アドレス、パブリック IP アドレス、E メール・サーバーなどがあります。

オールインワン・システムでのネットワーク設定の変更

オールインワン・システムでネットワーク設定を変更できます。オールインワン・システムには、1 つのシステムにインストールされているすべての IBM Security QRadar コンポーネントが含まれています。

始める前に

- QRadar コンソールへのローカル接続が必要です。
- デプロイされていない変更がないことを確認してください。
- デプロイメント内のボックスの IP アドレス・ホスト名を変更する場合、デプロイメントから IP アドレス・ホスト名を削除する必要があります。
- このシステムが HA ペアの一部である場合、いずれのネットワーク設定を変更する前にも、まず HA を無効にする必要があります。
- 変更するシステムがこのコンソールである場合、続行する前にデプロイメント内のすべてのホストを削除する必要があります。

手順

1. root ユーザーとしてログインします。
2. 次のコマンドを入力します。

   ```
   qchange_netsetup
   ```

3. ウィザードの指示に従って、構成を完了してください。

   ネットワーク設定を構成する際に役立つ説明と注意事項を次の表に示します。

表 *14.* オールインワン *QRadar* コンソールのネットワーク設定の説明

ネットワーク設定	説明
ホスト名	完全修飾ドメイン名
セカンダリー DNS サーバー・アドレス	オプション

表 14. オールインワン *QRadar* コンソールのネットワーク設定の説明 (続き)

ネットワーク設定	説明
ネットワーク・アドレス変換 (NAT) を使用するネットワークのパブリック IP アドレス	オプション サーバーへのアクセス (通常は、異なるネットワークまたはインターネットからのアクセス) で使用されます。 ご使用のネットワークのネットワーク・アドレス変換 (NAT) サービスまたはネットワークのファイアウォール設定を使用して構成されます。(NAT は、あるネットワーク内の IP アドレスを、別のネットワーク内の異なる IP アドレスに変換します)。
E メール・サーバー名	E メール・サーバーがない場合は `localhost` を使用します。

QRadar が要求された変更を処理すると、一連のメッセージが表示されます。要求された変更の処理後に、QRadar システムは自動でシャットダウンおよび再始動されます。

マルチシステム・デプロイメントでの QRadar コンソールのネットワーク設定の変更

マルチシステム IBM Security QRadar デプロイメントでネットワーク設定を変更するには、すべての管理対象ホストを削除し、ネットワーク設定を変更し、管理対象ホストを再び追加してからコンポーネントを再度割り当てます。

始める前に

- QRadar コンソールへのローカル接続が必要です。

手順

1. 管理対象ホストを削除するには、QRadar にログインします。

   `https://`*`IP_Address_QRadar`*

   「ユーザー名」は `admin` です。

   a. 「管理」タブをクリックします。
   b. 「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。
   c. 削除する管理対象ホストを選択します。
   d. 「デプロイメント・アクション」 > 「ホストの削除」を選択します。
   e. 「管理」タブで、「変更のデプロイ」をクリックします。
2. コマンド `qchange_netsetup` を入力します。
3. ウィザードの指示に従って、構成を完了してください。

   ネットワーク設定を構成する際に役立つ説明と注意事項を次の表に示します。

表 15. マルチシステム *QRadar* コンソールデプロイメントのネットワーク設定の説明：

ネットワーク設定	説明
ホスト名	完全修飾ドメイン名
セカンダリー DNS サーバー・アドレス	オプション
ネットワーク・アドレス変換 (NAT) を使用するネットワークのパブリック IP アドレス	オプション サーバーへのアクセス (通常は、異なるネットワークまたはインターネットからのアクセス) で使用されます。 ご使用のネットワークのネットワーク・アドレス変換 (NAT) サービスまたはネットワークのファイアウォール設定を使用して構成されます。(NAT は、あるネットワーク内の IP アドレスを、別のネットワーク内の異なる IP アドレスに変換します)。
E メール・サーバー名	E メール・サーバーがない場合は `localhost` を使用します。

インストール・パラメーターを構成すると、一連のメッセージが表示されます。このインストール・プロセスは、完了までに数分かかる場合があります。

4. 管理対象ホストの再追加および再割り当てを行うには、QRadar にログインします。

   `https://`*`IP_Address_QRadar`*

   「ユーザー名」は `admin` です。

   a. 「管理」タブをクリックします。
   b. 「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。
   c. 「デプロイメント・アクション」 > 「ホストの追加」をクリックします。
   d. ウィザードの指示に従って、ホストを追加します。

      サーバーのパブリック IP アドレスを構成するため、「ネットワーク・アドレス変換」オプションを選択します。この IP アドレスは、サーバーへのアクセス (通常は、異なるネットワークまたはインターネットからのアクセス) で使用されるセカンダリー IP アドレスです。パブリック IP アドレスは、多くの場合、ご使用のネットワークのネットワーク・アドレス変換 (NAT) サービスまたはネットワークのファイアウォール設定を使用して構成されます。NAT は、あるネットワーク内の IP アドレスを、別のネットワーク内の異なる IP アドレスに変換します。

5. ご使用の QRadar コンソールではないすべてのコンポーネントを、管理対象ホストに再割り当てします。

   a. 「管理」タブをクリックします。
   b. 「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。
   c. 再割り当てするホストを選択します。

d. 「デプロイメント・アクション」 > 「ホスト接続の編集」をクリックします。

e. 「接続の変更 **(Modify Connection)**」ウィンドウでソース・ホストの IP アドレスを入力します。

NIC 交換後のネットワーク設定の更新

統合システム・ボードまたはスタンドアロン NIC (ネットワーク・インターフェース・カード) を交換した場合は、ハードウェアが引き続き作動可能であるようにするため、IBM Security QRadar ネットワーク設定を更新する必要があります。

このタスクについて

ネットワーク設定ファイルには、設置された NIC ごとに行のペアが 1 つと、取り外された NIC ごとに行のペアが 1 つずつ含まれています。取り外した NIC の行を削除してから、設置した NIC の名前を変更する必要があります。

ネットワーク設定ファイルは、以下の例のようになります。ここで、*NAME="eth0"* は取り外された NIC、*NAME="eth4"* は設置された NIC です。

```
# PCI device 0x14e4:0x163b (bnx2)
SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?*",
ATTR{address}=="78:2a:cb:23:1a:2f", ATTR{type}=="1",
KERNEL=="eth*", NAME="eth0"

# PCI device 0x14e4:0x163b (bnx2)
SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?*",
ATTR{address}=="78:2a:cb:23:1a:2f", ATTR{type}=="1",
KERNEL=="eth*", NAME="eth0"

# PCI device 0x14e4:0x163b (bnx2)
SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?*",
ATTR{address}=="78:2a:cb:23:1a:2f", ATTR{type}=="1",
KERNEL=="eth*", NAME="eth4"

# PCI device 0x14e4:0x163b (bnx2)
SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?*",
ATTR{address}=="78:2a:cb:23:1a:2f", ATTR{type}=="1",
KERNEL=="eth*", NAME="eth4"
```

手順

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

   ユーザー名は `root` です。

2. 次のコマンドを入力します。

   ```
   cd /etc/udev/rules.d/
   ```

3. ネットワーク設定ファイルを編集するには、以下のコマンドを入力します。

   ```
   vi 70-persistent-net.rules
   ```

4. 取り外された NIC に対応する行のペア (`NAME="eth0"`) を削除します。

5. 新しく設置した NIC について `Name=<eth>` の値を名前変更します。

   例: `NAME="eth4"` を `NAME="eth0"` に名前変更します。

6. ファイルを保存して閉じます。
7. コマンド `reboot` を入力します。

第 11 章 問題のトラブルシューティング

トラブルシューティングとは、問題を解決するための体系的な方法です。トラブルシューティングの目的は、想定どおりに機能しない理由とその問題の解決方法を判別することです。

お客様やカスタマー・サポートが問題を解決しやすくするために、以下の表を確認してください。

表 16. 問題の発生を防止するためのトラブルシューティング・アクション

アクション	説明
入手可能なフィックスパック、サービス・レベル、およびプログラム一時修正 (PTF) をすべて適用してください。	問題を修正するために製品フィックスが入手可能な場合があります。
構成がサポート対象であることを確認してください。	ソフトウェア要件とハードウェア要件を確認してください。
IBM サポート・ポータル (http://www.ibm.com/support/entry/portal) から製品を選択してから「サポート技術情報検索」ボックスにエラー・メッセージ・コードを入力することによって、エラー・メッセージ・コードを調べます。	エラー・メッセージは、問題の原因となっているコンポーネントを識別するために役立つ重要な情報を提供します。
問題を再現して、単純なエラーではないことを確認します。	製品でサンプルが使用できる場合には、そのサンプル・データを使用して、問題の再現を試みてください。
インストール・ディレクトリー構造とファイルの許可を確認してください。	インストール場所には、適切なファイル構造とファイル許可が含まれていなければなりません。 例えば、製品でログ・ファイルへの書き込みアクセス権限が必要な場合、対象ディレクトリーに正しい許可があることを確認します。
関連する資料 (リリース・ノート、技術情報、実証済み操作に関する資料など) を確認してください。	IBM 知識ベースを検索し、問題が既知のものか、回避策があるかどうか、あるいは既に解決済みで文書化されているかを確認します。
コンピューティング環境の最近の変更を確認します。	新しいソフトウェアをインストールしたことで互換性の問題が発生する場合があります。

それでもまだ問題の解決を要する場合は、診断データを収集する必要があります。このデータは、IBM 技術サポート担当者が効率的にトラブルシューティングを行い、ユーザーの問題の解決を支援するために必要となります。また、ユーザー自身で診断データを収集し、分析することもできます。

関連概念:

3 ページの『QRadar コンポーネント』
IBM Security QRadar は、ネットワーク上のデバイスやアプリケーションによって

使用されるログ・ソースからのイベント・データを統合します。

トラブルシューティング・リソース

トラブルシューティング・リソースとは、製品の使用時に発生する問題の解決に役立つ情報源のことを指します。提供されているリソース・リンクの多くは、ショート・ビデオ・デモンストレーションでもご覧になれます。

ビデオ版を見るには、Google 検索エンジンか YouTube ビデオ・コミュニティーで「トラブルシューティング」を検索します。

関連概念:

65 ページの『QRadar のログ・ファイル』
IBM Security QRadar のログ・ファイルを使用して問題のトラブルシューティングに役立てます。

サポート・ポータル

IBM サポート・ポータルは、すべての IBM システム、ソフトウェア、およびサービスについてのすべての技術サポート・ツールと情報が統合され、集中化されたビューです。

IBM サポート・ポータルを使用して、1 箇所からすべての IBM サポート・リソースにアクセスします。各ページを調整して、問題の予防と迅速な問題解決に必要な情報やリソースに焦点を当てることができます。IBM サポート・ポータルをさらに理解するには、デモ・ビデオ (https://www.ibm.com/blogs/SPNA/entry/the_ibm_support_portal_videos) を参照してください。

IBM サポート・ポータル (http://www.ibm.com/support/entry/portal) からご使用の製品を選択して、必要な IBM Security QRadar コンテンツを見つけてください。

サービス・リクエスト

サービス・リクエストは、問題管理レコード (PMR) とも呼ばれます。IBM ソフトウェア技術サポートに診断情報を送信するには、いくつかの方法があります。

サービス・リクエストを開いたり、テクニカル・サポートと情報を交換したりするには、IBM ソフトウェア・サポートの技術サポートとの情報交換ページ (http://www.ibm.com/software/support/exchangeinfo.html) にアクセスしてください。サービス・リクエストは、サービス・リクエスト (PMR) ツール (http://www.ibm.com/support/entry/portal/Open_service_request) や、情報交換ページで詳述されているサポート対象の他のいずれかの方法を使用して、直接送信することもできます。

Fix Central

Fix Central は、システムのソフトウェア、ハードウェア、およびオペレーティング・システム用のフィックスおよび更新を提供します。

Fix Central (http://www.ibm.com/support/fixcentral) のプルダウン・メニューを使用して、製品フィックスに移動します。 Fix Central ヘルプ (http://www.ibm.com/systems/support/fixes/en/fixcentral/help/getstarted.html) を表示することもできます。

知識ベース

多くの場合、IBM 知識ベースを検索することで問題の解決方法が見つかります。使用可能なリソース、サポート・ツール、および検索方式を使用して、最適の結果を得ることができます。

以下の知識ベースを使用して有用な情報を検索します。

技術情報と **APAR**

IBM サポート・ポータル (http://www.ibm.com/support/entry/portal) で、技術情報と APAR (問題報告書) を検索することができます。

IBM マストヘッド検索

どの ibm.com ページでも、上部の「検索」フィールドに検索ストリングを入力することで、IBM マストヘッド検索を使用できます。

外部の検索エンジン

外部の検索エンジン (Google、Yahoo、Bing など) を使用して、コンテンツを検索します。外部検索エンジンを使用すると、ibm.com® ドメイン以外の情報が結果に含まれる可能性が高くなります。ただし、ibm.com 以外のニュースグループ、フォーラム、およびブログで IBM 製品の問題解決に関して役立つ情報が見つかる場合があります。

ヒント**:** IBM 製品に関する情報を検索する場合は、「IBM」と製品の名前を検索に含めてください。

QRadar のログ・ファイル

IBM Security QRadar のログ・ファイルを使用して問題のトラブルシューティングに役立てます。

現行セッションのログ・ファイルを個別に確認したり、後で確認するためにログ・ファイルを収集したりできます。

QRadar のログ・ファイルを確認するには、以下の手順を実行します。

1. エラーや例外のトラブルシューティングを容易にするために以下のログ・ファイルを確認します。
   - `/var/log/qradar.log`
   - `/var/log/qradar.error`
2. 詳細が必要な場合は、以下のログ・ファイルを確認してください。
   - /var/log/qradar-sql.log
   - /opt/tomcat6/logs/catalina.out
   - /var/log/qflow.debug

3. 「管理」 > 「システムおよびライセンス管理」 > 「アクション」 > 「ログ・ファイルの収集」を選択してすべてのログを確認します。

関連概念:

64 ページの『トラブルシューティング・リソース』
トラブルシューティング・リソースとは、製品の使用時に発生する問題の解決に役立つ情報源のことを指します。提供されているリソース・リンクの多くは、ショート・ビデオ・デモンストレーションでもご覧になれます。

QRadar で使用される共通ポートとサーバー

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ポートを確認します。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オープンする必要があるポートを判別することができます。

ここでは、QRadar の listen ポートについて説明します。listen ポートは、QRadar システム上で iptables が有効になっている場合のみ使用することができます。

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、暗号化を使用することにより、SSH 経由でポート 22 をトンネリングできます。セキュリティー上の理由から、管理対象ホストからコンソールへの SSH トンネルをセットアップすることはできませんが、コンソールから管理対象ホストへの SSH トンネルをセットアップすることはできます。管理対象ホストの公開鍵は、コンソール側の許可された鍵ファイルに追加されません。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 (Event Processor)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 コレクターは、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。

割り当て済みポート番号、説明、プロトコル、ポートのシグナル方向についての情報は、特に明記されていない限り、すべての IBM Security QRadar 製品に適用されます。

QRadar が使用中のポートの検索

netstat コマンドを使用して、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. コンピューターが listen 中の TCP ポートと UDP ポートおよびアクティブな接続をすべて表示するには、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。

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。

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。

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。

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]

[ラ行]

A

F

L

Q

U

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