

IBM Security QRadar Risk Manager
バージョン 7.2.6

インストール・ガイド

The IBM logo, consisting of the letters "IBM" in a bold, sans-serif font, with each letter formed by eight horizontal stripes of varying lengths.

注記

本書および本書で紹介する製品を使用する前に、31 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 Risk Manager
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

© Copyright IBM Corporation 2012, 2015.

目次

IBM Security QRadar Risk Manager のインストールの概要	v
第 1 章 IBM Security QRadar Risk Manager のインストールの準備	1
第 2 章 インストールの前に	3
ネットワーク設定の識別	3
ファイアウォールのポート・アクセスの構成	3
IBM Security QRadar Risk Manager でサポートされない機能	4
第 3 章 追加のハードウェア要件	5
第 4 章 追加のソフトウェア要件	7
第 5 章 サポート対象の Web ブラウザー	9
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	9
第 6 章 IBM Security QRadar Risk Manager アプライアンスのインストール	11
アプライアンスの準備	11
IBM Security QRadar Risk Manager ユーザー・インターフェースへのアクセス	12
IPv4 のネットワーク・パラメーター情報	12
IBM Security QRadar Risk Manager のインストール	12
IBM Security QRadar SIEM コンソールへの IBM Security QRadar Risk Manager の追加	13
Web ブラウザー・キャッシュのクリア	15
第 7 章 Risk Manager のユーザー・ロール	17
Risk Manager のユーザー・ロールの割り当て	17
第 8 章 「リスク」タブのトラブルシューティング	19
管理対象ホストの削除	19
第 9 章 管理対象ホストとしての IBM Security QRadar Risk Manager の再追加	21
第 10 章 リカバリー・パーティションからの IBM Security QRadar Risk Manager の再インストール	23
「出荷時状態で再インストール (Factory re-install)」を使用した IBM Security QRadar Risk Manager の再インストール	23
第 11 章 ネットワーク設定の変更	25
管理対象ホストの削除	25
ネットワーク設定の変更	25
管理対象ホストとしての IBM Security QRadar Risk Manager の再追加	26
第 12 章 データのバックアップおよびリストア	27
データのバックアップとリストアの前提条件	27
データのバックアップ	28
データのリストア	28
特記事項	31
商標	32
プライバシー・ポリシーに関する考慮事項	33

IBM Security QRadar Risk Manager のインストールの概要

本書は、IBM® Security QRadar® Risk Manager と一緒に使用することを意図しています。QRadar Risk Manager は、デバイス構成のモニター、ネットワーク環境の変更のシミュレート、およびネットワーク内のリスクと脆弱性の優先順位付けを行うために使用するアプライアンスです。

本書には、QRadar Risk Manager をインストールする手順および IBM Security QRadar SIEM コンソール に管理対象ホストとして QRadar Risk Manager を追加する手順が記載されています。

QRadar Risk Manager アプライアンスには、ソフトウェアと 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。また、QRadar Risk Manager ソフトウェアをご使用のハードウェアにインストールすることもできます。

対象読者

本書は、ネットワーク内に QRadar Risk Manager システムのインストールおよび構成を行うネットワーク管理者を対象としています。

管理者には、ネットワークおよび Linux システムの実用的な知識が必要です。

技術文書

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 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:

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。ライセンサーは、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 IBM Security QRadar Risk Manager のインストールの準備

IBM Security QRadar Risk Manager アプライアンスを管理対象ホストとして IBM Security QRadar SIEM コンソールにインストールします。1 つの QRadar Risk Manager のみが、QRadar コンソールに存在できます。

QRadar コンソールと QRadar Risk Manager は同じインストール・プロセスおよび ISO イメージを使用します。QRadar コンソールと QRadar Risk Manager をインストールした後、「管理」タブの「システムおよびライセンス管理」ツールを使用して QRadar Risk Manager を管理対象ホストとして追加します。QRadar Risk Manager アプライアンスには、QRadar Risk Manager ソフトウェアと 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。

第 2 章 インストールの前に

IBM Security QRadar Risk Manager をインストールする前に、IBM Security QRadar SIEM コンソールのインストール・プロセスを完了する必要があります。QRadar SIEM および QRadar Risk Manager を同じネットワーク・スイッチにインストールすることをお勧めします。

QRadar SIEM のインストール方法 (ハードウェア要件およびソフトウェア要件を含む) については、「*IBM Security QRadar SIEM 管理ガイド*」を参照してください。

QRadar Risk Manager は 64 ビット・アプライアンスであるため、ご使用のオペレーティング・システムに適したインストール・ソフトウェアをダウンロードするようにしてください。

ネットワーク設定の識別

ネットワーク設定に関する情報を収集してからインストール・プロセスを開始する必要があります。

ネットワーク設定について以下の情報を収集します。

- ホスト名
- IP アドレス
- ネットワーク・マスク・アドレス
- サブネット・マスク
- デフォルトのゲートウェイ・アドレス
- プライマリー・ドメイン・ネーム・システム (DNS) サーバーのアドレス
- セカンダリー DNS サーバー (オプション) のアドレス
- ネットワーク・アドレス変換 (NAT) の E メール・サーバー名を使用するネットワークのパブリック IP アドレス
- E メール・サーバー名
- Network Time Protocol (NTP) サーバー (コンソールのみ) 名またはタイム・サーバー名

ファイアウォールのポート・アクセスの構成

IBM Security QRadar SIEM コンソールと IBM Security QRadar Risk Manager の間にあるファイアウォールは、特定のポートでのトラフィックを許可する必要があります。

QRadar SIEM コンソールと QRadar Risk Manager の間にあるファイアウォールでは以下のポートでのトラフィックを許可するようにしてください。

- ポート 443 (HTTPS)
- ポート 22 (SSH)
- ポート 37 UDP (Time)

IBM Security QRadar Risk Manager でサポートされない機能

QRadar Risk Manager でサポートされない機能を認識することは重要です。

以下の機能は、QRadar Risk Manager でサポートされていません。

- 高可用性 (HA)
- Border Gateway Protocol (BGP)、Open Shortest Path First (OSPF)、または Routing Information Protocol (RIP) の動的ルーティング
- IPv6
- 不連続のネットワーク・マスク
- 負荷分散ルーティング
- リファレンス・マップ
- ストア・アンド・フォワード

第 3 章 追加のハードウェア要件

IBM Security QRadar Risk Manager をインストールするには、追加のハードウェアが必要です。

QRadar Risk Manager システムをインストールするには、以下のハードウェア・コンポーネントにアクセスする必要があります。

- モニターおよびキーボード
- 無停電電源装置 (UPS)

無停電電源装置 (UPS) を使用して、データを保管する QRadar Risk Manager のインストール済み環境を保護してください。UPS の仕様により、QRadar Risk Manager データ (コンソール、イベント・プロセッサ、および QRadar QFlow Collector で保管されたデータ) は電源障害時にも保持されるようになります。

第 4 章 追加のソフトウェア要件

IBM Security QRadar Risk Manager をインストールするには、追加のソフトウェアが必要です。

QRadar Risk Manager ユーザー・インターフェースへのアクセスに使用するデスクトップ・システムに、以下のソフトウェアをインストールする必要があります。

- Java™ ランタイム環境
- Adobe Flash バージョン 10 以上

第 5 章 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 1. 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 ビット版の Microsoft Internet Explorer (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こと)	10.0 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。

第 6 章 IBM Security QRadar Risk Manager アプライアンスのインストール

IBM Security QRadar Risk Manager デプロイメントには IBM Security QRadar SIEM コンソールおよび QRadar Risk Manager アプライアンスが管理対象ホストとして含まれます。

QRadar Risk Manager のインストールには以下のステップが含まれます。

1. アプライアンスの準備。
2. QRadar Risk Manager のインストール。
3. QRadar への QRadar Risk Manager の追加。

アプライアンスの準備

IBM Security QRadar Risk Manager アプライアンスをインストールする前にアプライアンスの準備をする必要があります。

始める前に

必要なハードウェアをすべてインストールし、アクティベーション・キーを用意する必要があります。アクティベーション・キーは、IBM から受け取る、24 桁で 4 つの部分からなる英数字ストリングです。アクティベーション・キーは以下の場所にあります。

- ステッカーに印刷され、アプライアンスに貼られています。
- パッキング・スリップに記載され、すべてのアプライアンスが関連キーとともにリストされています。

入力エラーを防ぐため、文字 O と数字 0 (ゼロ) は同じものとして扱われます。また、文字 I と数字 1 (一) についても同様です。

QRadar Risk Manager アプライアンスのアクティベーション・キーがない場合は、お客様サポート (www.ibm.com/support/) にお問い合わせください。

アプライアンスについて詳しくは、「*IBM Security QRadar Hardware Installation Guide*」を参照してください。

手順

1. 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。
2. システムの電源をオンにしてログインします。ユーザー名は root です (大/小文字を区別します)。
3. **Enter** キーを押します。
4. ウィンドウ内の情報を確認します。各ウィンドウで文書の最後に達するまでスペース・バーを押します。
5. ご使用条件に同意するには yes と入力し、Enter キーを押します。

6. アクティベーション・キーを入力して、Enter キーを押します。

IBM Security QRadar Risk Manager ユーザー・インターフェースへのアクセス

IBM Security QRadar Risk Manager は、URL、ユーザー名、およびパスワードに関するデフォルトのログイン情報を使用します。

IBM Security QRadar SIEM コンソールから QRadar Risk Manager にアクセスします。QRadar コンソールにログインする際は、以下の表の情報を参照してください。

表 2. QRadar Risk Manager のデフォルトのログイン情報

ログイン情報	デフォルト
URL	https://<IP address>。ここで、<IP address> は QRadar コンソールの IP アドレスです。
ユーザー名	管理
パスワード	インストール・プロセスで QRadar Risk Manager に割り当てられたパスワード。
ライセンス・キー	デフォルトのライセンス・キーを使用すると、システムに 5 週間アクセスすることができます。

IPv4 のネットワーク・パラメーター情報

インターネット・プロトコル・バージョン 4 (IPv4) ネットワーク設定のネットワーク情報は、IBM Security QRadar Risk Manager のインストール時またはネットワーク設定の変更時に必要となります。

ネットワーク情報は、QRadar Risk Manager のインストール時、再インストール時、またはネットワーク設定の変更が必要な場合に必要となります。

パブリック IP ネットワーク設定はオプションです。このセカンダリー IP アドレスはサーバーへのアクセス (通常は別のネットワークまたはインターネットからのアクセス) に使用され、ネットワーク管理者によって管理されます。多くの場合、パブリック IP アドレスはネットワーク上のネットワーク・アドレス交換 (NAT) サービスまたは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。

IBM Security QRadar Risk Manager のインストール

アプライアンスを準備した後、IBM Security QRadar Risk Manager をインストールできます。

始める前に

QRadar Risk Manager をインストールする前に、準備ステップを完了する必要があります。

手順

1. セットアップのタイプとして「標準 (normal)」を選択します。「次へ」を選択して、Enter キーを押します。
2. タイム・ゾーンの大陸または領域を選択します。「次へ」を選択して、Enter キーを押します。
3. タイム・ゾーンの地域を選択します。「次へ」を選択して、Enter キーを押します。
4. インターネット・プロトコルのバージョンを選択します。「次へ」を選択して、Enter キーを押します。
5. 管理インターフェースとして指定するインターフェースを選択します。「次へ」を選択して、Enter キーを押します。
6. ホスト名、IP アドレス、ネットワーク・マスク、ゲートウェイ、プライマリー DNS、セカンダリー DNS、パブリック IP、および Eメール・サーバーを入力します。ネットワーク・パラメーター情報については、12 ページの『IPv4 のネットワーク・パラメーター情報』を参照してください。
7. 「次へ」を選択して、Enter キーを押します。
8. パスワードを入力して、QRadar Risk Manager のルート・パスワードを構成します。
9. 「次へ」を選択して、Enter キーを押します。
10. 確認のために新規パスワードを再入力します。「終了」を選択して、Enter キーを押します。通常、このプロセスには数分間かかります。

IBM Security QRadar SIEM コンソールへの IBM Security QRadar Risk Manager の追加

IBM Security QRadar Risk Manager を管理対象ホストとして IBM Security QRadar SIEM コンソールに追加する必要があります。

始める前に

圧縮を有効にする場合、各管理対象ホストの最小バージョンを QRadar コンソール V7.1 または QRadar Risk Manager V7.1 にする必要があります。

コンソールが NAT されているデプロイメント環境に、NAT されていない管理対象ホストを追加するには、QRadar コンソール を NAT されたホストに変更する必要があります。コンソールを変更してから管理対象ホストをデプロイメントに追加してください。詳細については、*IBM Security QRadar SIEM 管理ガイド* を参照してください。

手順

1. Web ブラウザーを開きます。
2. URL `https://<IP Address>` を入力します。ここで、<IP Address> は QRadar コンソールの IP アドレスです。
3. ユーザー名とパスワードを入力します。
4. 「管理」タブをクリックします。

5. 「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。
6. 「システムおよびライセンス管理」 ウィンドウで、「デプロイメント・アクション」をクリックしてから、「ホストの追加」を選択します。
7. 「次へ」をクリックします。
8. 以下のパラメーターの値を入力します。

オプション	説明
ホスト IP	QRadar Risk Manager の IP アドレス。
ホスト・パスワード	ホストの root パスワード。
ホスト・パスワードの確認	パスワードの確認。
ホスト接続の暗号化	ホストの SSH 暗号化トンネルを作成します。2 つの管理対象ホストの間で暗号化を有効にするには、各管理対象ホストで QRadar コンソール V7.1 または QRadar Risk Manager V7.1 が実行されている必要があります。
暗号化圧縮	2 つの管理対象ホストの間でデータ圧縮を有効にします。
ネットワーク・アドレス変換	管理対象ホストに対して NAT を有効にするには、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。詳しくは、「 <i>IBM Security QRadar SIEM 管理ガイド</i> 」を参照してください。

9. 「ネットワーク・アドレス変換」 チェック・ボックスを選択した場合は、NAT パラメーターの値を入力する必要があります。

オプション	説明
NAT グループ	この管理対象ホストで使用されるネットワーク。 管理対象ホストが QRadar コンソールと同じサブネット上にある場合、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 QRadar 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。
パブリック IP	管理対象ホストのパブリック IP アドレス。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内の他の管理対象ホストと通信します。

10. 「追加」をクリックします。このプロセスには、数分かかることがあります。デプロイメントに変更が含まれている場合は、すべての変更をデプロイする必要があります。
11. 「管理」タブから、「拡張」 > 「すべての構成のデプロイ」をクリックします。

次のタスク

Web ブラウザー・キャッシュをクリアして、QRadar コンソールにログインします。これで「リスク」タブが使用可能になりました。

Web ブラウザー・キャッシュのクリア

IBM Security QRadar SIEM コンソールの「リスク」タブにアクセスするには、Web ブラウザー・キャッシュをクリアしておく必要があります。

始める前に

開いている Web ブラウザーは 1 つのみであることを確認してください。複数のブラウザを開いている場合は、キャッシュが正しくクリアされないおそれがあります。

Mozilla Firefox Web ブラウザーを使用する場合は、Microsoft Internet Explorer Web ブラウザーのキャッシュもクリアする必要があります。

手順

1. Web ブラウザーを開きます。
2. Web ブラウザー・キャッシュをクリアします。手順については、ご使用の Web ブラウザーの資料を参照してください。

第 7 章 Risk Manager のユーザー・ロール

「リスク」タブへのアクセスが必要なユーザーには、Risk Manager のユーザー・ロールを割り当てる必要があります。

ユーザー・アカウントは、ユーザーのデフォルトのパスワード、および E メール・アドレスを定義します。ユーザー・ロールとセキュリティー・プロファイルを新規ユーザー・アカウントごとに割り当てる必要があります。

IBM Security QRadar Risk Manager 機能へのアクセスを組織内のユーザーに許可するには、適切なユーザー・ロール権限を割り当てる必要があります。デフォルトでは、QRadar コンソールには、デフォルトの管理ロール (QRadar Risk Manager 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。

ユーザー・ロールの作成および管理については、「*IBM Security QRadar SIEM 管理ガイド*」を参照してください。

Risk Manager のユーザー・ロールの割り当て

「リスク」タブへのアクセスが必要なユーザーに Risk Manager のユーザー・ロール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. 「ユーザー管理」ペインで、「ユーザー・ロール」アイコンをクリックします。
4. 編集するユーザー・ロールの横にある「編集」アイコンをクリックします。
5. 「リスク・マネージャー (Risk Manager)」チェック・ボックスを選択します。
6. 「次へ」をクリックします。「ログ・アクティビティー」権限を持つユーザー・ロールに Risk Manager を追加する場合は、ユーザー・ロールがアクセスできるログ・ソースを定義してください。ログ・ソース・グループ全体を追加するには、「ログ・ソース・グループ」ペインの「追加」アイコンをクリックします。複数のログ・ソースを選択するには、Ctrl キーを押したまま、追加する各ログ・ソースを選択します。
7. 「戻る」をクリックします。
8. 「管理」タブ・メニューから、「変更のデプロイ」をクリックします。

第 8 章 「リスク」 タブのトラブルシューティング

「リスク」タブが正しく表示されないかアクセス不能の場合は、トラブルシューティングをすることができます。

「リスク」タブが正しく表示されないかアクセス不能の場合は、IBM Security QRadar Risk Manager を削除し、管理対象ホストとして再追加してください。

管理対象ホストの削除

ネットワーク設定を変更する場合や「リスク」タブに問題がある場合、IBM Security QRadar Risk Manager 管理対象ホストを IBM Security QRadar SIEM コンソールから削除できます。

手順

1. QRadar コンソールに管理者としてログインします。

`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、インストール時に入力された、`root` ユーザー・アカウントのパスワードです。

2. 「管理」タブをクリックします。
3. 「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。
4. ホスト・テーブルで、削除する QRadar Risk Manager ホストをクリックし、そして「デプロイメント・アクション」 > 「ホストの削除」をクリックします。
5. 「管理」タブのメニュー・バーで、「変更のデプロイ」をクリックします。
6. Web ブラウザーを最新表示します。

第 9 章 管理対象ホストとしての IBM Security QRadar Risk Manager の再追加

IBM Security QRadar Risk Manager は削除した後に、管理対象ホストとして再追加できます。

手順

1. 「管理」タブで、「システムおよびライセンス管理」 > 「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。
2. ホストの IP アドレスとパスワードを入力します。
3. 「追加」をクリックします。

管理対象ホストが追加されるまで、数分待つ必要があります。

4. 「システムおよびライセンス管理」を閉じます。
5. 「管理」タブのツールバーで、「拡張」 > 「すべての構成のデプロイ」をクリックします。
6. 「OK」をクリックします。

第 10 章 リカバリー・パーティションからの IBM Security QRadar Risk Manager の再インストール

IBM Security QRadar Risk Manager をリカバリー・パーティションの IBM Security QRadar SIEM/IBM Security QRadar SIEM コンソールの ISO から再インストールすると、システムがリストアされて出荷時のデフォルト構成に戻ります。この場合、現在の構成とデータ・ファイルは上書きされます。

以下の情報は、QRadar Risk Manager アプライアンス上での QRadar Risk Manager の新規インストールか、QRadar Risk Manager の新規インストール済み環境からのアップグレードに適用されます。QRadar Risk Manager をインストールすると、インストーラー (QRadar コンソールの ISO) 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 Risk Manager を再インストールして、QRadar Risk Manager を出荷時のデフォルト状態にリストアすることができます。

注: QRadar Risk Manager のインストール後にソフトウェアをアップグレードした場合は、ISO ファイルが新しいバージョンに置き換えられます。

QRadar Risk Manager アプライアンスをリブートすると、ソフトウェアを再インストールするオプションが提示されます。QRadar コンソールと QRadar Risk Manager は同じ ISO インストール・ファイルを使用するため、QRadar コンソールの ISO 名が表示されます。

プロンプトに回答しないで 5 秒経過すると、システムは通常のようにリブートされ、構成とデータ・ファイルが維持されます。QRadar コンソールの ISO の再インストールを選択すると、警告メッセージが表示され、ソフトウェアを再インストールすることを確定する必要があります。確定すると、インストーラーが実行されます。プロンプトに従ってインストール・プロセスを実行できます。

ハード・ディスク障害が発生すると、リカバリー・パーティションは使用できなくなるため、リカバリー・パーティションから再インストールすることはできません。ハード・ディスク障害が発生した場合は、お客様サポートにお問い合わせください。

「出荷時状態で再インストール (Factory re-install)」を使用した IBM Security QRadar Risk Manager の再インストール

ファクトリー・インストール・オプションを使用して、IBM Security QRadar Risk Manager アプライアンスを再始動したり、再インストールしたりすることができます。

始める前に

アクティベーション・キーを用意してください。アクティベーション・キーは、IBM から受け取る、24 桁で 4 つの部分からなる英数字ストリングです。このキーは、以下の場所にあります。

- ステッカーに印刷され、アプライアンスに貼られています。
- パッキング・スリップに記載され、すべてのアプライアンスが関連キーとともにリストされています。

入力エラーを防ぐため、文字 O と数字 0 (ゼロ) は同じものとして扱われます。また、文字 I と数字 1 (一) についても同様です。

QRadar Risk Manager アプライアンスのアクティベーション・キーがない場合は、お客様サポート (www.ibm.com/support/) にお問い合わせください。

ソフトウェアのアクティベーション・キーにはシリアル番号は必要ありません。

手順

1. QRadar Risk Manager アプライアンスをリブートします。
2. 「出荷時状態で再インストール (Factory re-install)」を選択します。
3. flatten と入力して続行します。ハード・ディスクのパーティション分割と再フォーマットが行われ、OS がインストールされます。次に、QRadar Risk Manager が再インストールされます。フラット化プロセスが完了するまで待つ必要があります。このプロセスは、システムによっては数分かかることがあります。
4. SETUP と入力します。
5. root ユーザーとして QRadar Risk Manager にログインします。
6. ウィンドウ内の情報を確認します。各ウィンドウで文書の最後に達するまでスペース・バーを押します。ご使用条件に同意するには yes と入力し、Enter キーを押します。
7. アクティベーション・キーを入力して、Enter キーを押します。
8. ウィザードの説明に従います。

通常、このプロセスには数分間かかります。

9. Enter キーを押して、「OK」を選択します。
10. Enter キーを押して、「OK」を選択します。

第 11 章 ネットワーク設定の変更

IBM Security QRadar SIEM コンソールに接続している IBM Security QRadar Risk Manager アプライアンスのネットワーク設定を変更できます。

ネットワーク設定を変更する必要がある場合は、これらのタスクを次の順序で実行してください。

1. 管理対象ホストとしての QRadar Risk Manager を削除します。
2. ネットワーク設定を変更します。
3. QRadar Risk Manager を管理対象ホストとして再追加します。

管理対象ホストの削除

ネットワーク設定を変更する場合や「リスク」タブに問題がある場合、IBM Security QRadar Risk Manager 管理対象ホストを IBM Security QRadar SIEM コンソールから削除できます。

手順

1. QRadar コンソールに管理者としてログインします。

`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、インストール時に入力された、`root` ユーザー・アカウントのパスワードです。

2. 「管理」タブをクリックします。
3. 「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。
4. ホスト・テーブルで、削除する QRadar Risk Manager ホストをクリックし、そして「デプロイメント・アクション」 > 「ホストの削除」をクリックします。
5. 「管理」タブのメニュー・バーで、「変更のデプロイ」をクリックします。
6. Web ブラウザーを最新表示します。

ネットワーク設定の変更

IBM Security QRadar SIEM コンソールに接続している IBM Security QRadar Risk Manager アプライアンスのネットワーク設定を変更できます。

始める前に

ネットワーク設定を変更する前に、QRadar コンソールから QRadar Risk Manager 管理対象ホストを削除する必要があります。

手順

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

2. コマンド `qchange_netsetup` を入力します。
3. インターネット・プロトコルのバージョンを選択します。「次へ」を選択して、Enter キーを押します。ハードウェア構成に応じて、ウィンドウには最大 4 つのインターフェースが表示されます。物理リンクのある各インターフェースはプラス (+) 記号付きで表示されます。
4. 管理インターフェースとして指定するインターフェースを選択します。「次へ」を選択して、Enter キーを押します。
5. ホスト名、IP アドレス、ネットワーク・マスク、ゲートウェイ、プライマリー DNS、セカンダリー DNS、パブリック IP、および E メール・サーバーについて情報を入力します。ネットワーク情報については、12 ページの『IPv4 のネットワーク・パラメーター情報』を参照してください。
6. パスワードを入力して、QRadar Risk Manager のルート・パスワードを構成します。
7. 「次へ」を選択して、Enter キーを押します。
8. 確認のために新規パスワードを再入力します。「終了」を選択して、Enter キーを押します。通常、このプロセスには数分間かかります。

管理対象ホストとしての IBM Security QRadar Risk Manager の再追加

IBM Security QRadar Risk Manager は削除した後に、管理対象ホストとして再追加できます。

手順

1. 「管理」タブで、「システムおよびライセンス管理」 > 「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。
2. ホストの IP アドレスとパスワードを入力します。
3. 「追加」をクリックします。

管理対象ホストが追加されるまで、数分待つ必要があります。

4. 「システムおよびライセンス管理」を閉じます。
5. 「管理」タブのツールバーで、「拡張」 > 「すべての構成のデプロイ」をクリックします。
6. 「OK」をクリックします。

第 12 章 データのバックアップおよびリストア

コマンド・ライン・インターフェース (CLI) スクリプトを使用して、IBM Security QRadar SIEM コンソールの管理対象ホストに保管されているデータをバックアップできます。

データ障害やハードウェア障害がアプライアンスに発生したら、CLI スクリプトを使用して IBM Security QRadar Risk Manager をリストアすることができます。

バックアップ・スクリプトは QRadar Risk Manager に含まれており、crontab を使用してスケジュールできます。このスクリプトは午前 3:00 に QRadar Risk Manager データの日次アーカイブを自動的に作成します。デフォルトでは、QRadar Risk Manager は最新の 5 つのバックアップを保持します。ネットワーク・ストレージまたは接続しているストレージがある場合は、cron ジョブを作成して QRadar Risk Manager のバックアップ・アーカイブをネットワーク・ストレージ・ロケーションにコピーしてください。

バックアップ・アーカイブには以下のデータが含まれています。

- QRadar Risk Manager のデバイス構成
- 接続データ
- トポロジー・データ
- ポリシー・モニターの質問
- QRadar Risk Manager のデータベース表

QRadar Risk Manager Maintenance リリース 5 からこの現行リリースへのマイグレーションについては、「*IBM Security QRadar Risk Manager Migration Guide*」を参照してください。

データのバックアップとリストアの前提条件

データのバックアップとリストアを行う前に、データのバックアップ方法、保管方法、およびアーカイブ方法を理解する必要があります。

データ・バックアップの場所

データは /store/qrm_backups ローカル・ディレクトリーにバックアップされます。システムには、外部の SAN サービスまたは NAS サービスのマウント /store/backup が含まれる場合があります。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ます。長期保管は、Payment Card Industry (PCI) 標準などのコンプライアンス規制に関して必要となる場合があります。

アプライアンス・バージョン

アーカイブにバックアップを作成したアプライアンスのバージョンが保管されません。IBM Security QRadar Risk Manager アプライアンスでバックアップをリストアできるのは、バックアップが同じバージョンの場合のみです。

データ・バックアップの頻度およびアーカイブの情報

データの日次バックアップは午前 3:00 に作成されます。最新の 5 つのバックアップ・ファイルのみが保管されます。QRadar Risk Manager に十分な空き領域がある場合は、バックアップ・アーカイブが作成されます。

バックアップ・ファイルの形式

以下の形式を使用して、バックアップ・ファイルを保存します。

```
backup-<target date>-<timestamp>.tgz
```

<target date> は、バックアップ・ファイルが作成された日付です。

対象とする日付の形式は、<day>_<month>_<year> です。<timestamp> は、バックアップ・ファイルが作成された時刻です。

タイム・スタンプの形式は、<hour>_<minute>_<second> です。

データのバックアップ

自動バックアップが毎日午前 3:00 に実行されます。手動でバックアップ・プロセスを開始することもできます。

手順

1. SSH を使用して、root ユーザーとして IBM Security QRadar SIEM コンソールにログインします。
2. QRadar コンソールから SSH を使用して、root ユーザーとして QRadar Risk Manager にログインします。
3. 以下のコマンドを使用して、QRadar Risk Manager のバックアップを開始します。

```
/opt/qradar/bin/dbmaint/risk_manager_backup.sh
```

タスクの結果

このスクリプトはバックアップ・プロセスを開始するために使用され、開始されるまで数分かかることがあります。

以下のメッセージは、スクリプトによるバックアップの完了後に表示される出力の例です。

```
Fri Sep 11 10:14:41 EDT 2015  
- Risk Manager Backup complete,  
wrote /store/qrm_backups/backup-2015-09-11-10-14-39.tgz
```

データのリストア

リストア・スクリプトを使用して、QRadar Risk Manager バックアップからデータをリストアできます。

始める前に

QRadar Risk Manager アプライアンスとバックアップ・アーカイブは同じバージョンの QRadar Risk Manager である必要があります。リストア・スクリプトがアーカイブと QRadar Risk Manager 管理対象ホストの間にバージョンの差異を検出すると、エラーが表示されます。

このタスクについて

リストア・スクリプトを使用して、QRadar Risk Manager にリストアするアーカイブを指定します。このプロセスでは、QRadar Risk Manager 上のサービスを停止する必要があります。サービスを停止すると、すべての QRadar Risk Manager ユーザーがログオフし、複数のプロセスが停止します。

以下の表は、バックアップ・アーカイブをリストアするために使用できるパラメーターについて説明しています。

表 3. バックアップ・アーカイブを QRadar Risk Manager にリストアするために使用されるパラメーター

オプション	説明
-f	システム上にある QRadar Risk Manager のすべての既存データをリストア・ファイルのデータで上書きします。このパラメーターを選択すると、スクリプトにより構成ソース管理のすべての既存のデバイス構成をバックアップ・ファイルのデバイス構成で上書きできます。
-w	QRadar Risk Manager データをリストアする前にディレクトリーを削除しません。
-h	リストア・スクリプトのヘルプ。

手順

1. SSH を使用して、root ユーザーとして IBM Security QRadar SIEM コンソールにログインします。
2. QRadar SIEM コンソールから SSH を使用して、root ユーザーとして QRadar Risk Manager にログインします。
3. `service hostcontext stop` と入力して、`hostcontext` を停止します。
4. 以下のコマンドを入力して、バックアップ・アーカイブを QRadar Risk Manager にリストアします。

```
/opt/qradar/bin/risk_manager_restore.sh -r /store/qrm_backups/<backup>.
```

<backup> は、リストアする QRadar Risk Manager アーカイブです。

例: `backup-2012-09-11-10-14-39.tgz`。

5. `service hostcontext start` と入力して、`hostcontext` を始動します。

特記事項

本書は米国 IBM が提供する製品およびサービスについて作成したものです。

本書に記載の製品、サービス、または機能が日本においては提供されていない場合があります。日本で利用可能な製品、サービス、および機能については、日本 IBM の営業担当員にお尋ねください。本書で IBM 製品、プログラム、またはサービスに言及していても、その IBM 製品、プログラム、またはサービスのみが使用可能であることを意味するものではありません。これらに代えて、IBM の知的所有権を侵害することのない、機能的に同等の製品、プログラム、またはサービスを使用することができます。ただし、IBM 以外の製品とプログラムの操作またはサービスの評価および検証は、お客様の責任で行っていただきます。

IBM は、本書に記載されている内容に関して特許権 (特許出願中のものを含む) を保有している場合があります。本書の提供は、お客様にこれらの特許権について実施権を許諾することを意味するものではありません。実施権についてのお問い合わせは、書面にて下記宛先にお送りください。

〒103-8510
東京都中央区日本橋箱崎町19番21号
日本アイ・ビー・エム株式会社
法務・知的財産
知的財産権ライセンス渉外

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を提供し、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。その測定値が、一般に利用可能なシステムのも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認できません。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をお願いします。

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ます、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。

Adobe、Adobe ロゴ、PostScript、PostScript ロゴは、Adobe Systems Incorporated の米国およびその他の国における登録商標または商標です。

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。

Java およびすべての Java 関連の商標およびロゴは Oracle やその関連会社の米国およびその他の国における商標または登録商標です。



Microsoft、Windows、Windows NT および Windows ロゴは、Microsoft Corporation の米国およびその他の国における商標です。

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 は無効にできませんが、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。