IBM Security QRadar Incident Forensics
バージョン 7.3.0

QRadar Packet Capture クイック・リファレンス・ガイド

注記

本書および本書で紹介する製品をご使用になる前に、 7 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 V7.3.0 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 Incident Forensics
Version 7.3.0
QRadar Packet Capture Quick Reference 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

Packet Capture クイック・リファレンス・ガイドについて

本書は、IBM® QRadar® Packet Capture のインストールおよび構成に必要なクイック・リファレンス情報を提供します。QRadar Packet Capture は IBM Security QRadar によりサポートされています。

対象読者

QRadar Packet Capture のインストールを担当するシステム管理者は、ネットワーク・セキュリティーの概念とデバイスの構成に精通している必要があります。

技術資料

QRadar 製品ライブラリー内のIBM Security QRadar 製品資料を検索するには、essing IBM Security Documentation 技術情報 (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・セキュリティーには、企業内外からの不正アクセスの防止、検出、および対応によって、システムや情報を保護することが求められます。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 Packet Capture のアップグレード

QRadar Packet Capture V7.2.8 から V7.3.0 にアップグレードするには、累積ソフトウェア・フィックスパックを QRadar Packet Capture アプライアンスにインストールする必要があります。アプライアンスにインストールされているソフトウェアのバージョンは、ビルド 7.2.6.241 でなければなりません。

手順

1. 実行中のパケット・キャプチャーまたは検索アクティビティーがないことを確認します。
2. SSH を使用して、root ユーザーとしてシステムにログインします。
3. 7.3.0-QRadar-PCAP-build<build_number>.sfs フィックスパックを IBM Fix Central (http://www.ibm.com/support/fixcentral/) からダウンロードします。
4. フィックスパックを /tmp ディレクトリーにコピーします。

   /tmp ディレクトリー内の容量が限られている場合、十分な容量がある別の場所にフィックスパックをコピーしてください。
5. 以下のコマンドを入力して、/updates ディレクトリーを作成してください。

   ```
   mkdir -p /updates
   ```
6. **cd** コマンドを使用して、フィックスパック・ファイルをコピーしたディレクトリーに移動します。

   ```
   cd /tmp
   ```
7. 以下のコマンドを入力して、フィックスパック・ファイルを /updates ディレクトリーにマウントします。

   ```
   mount -o loop -t squashfs 7.3.0-QRadar-PCAP-build<build_number>.sfs
   /updates
   ```
8. フィックスパックのインストーラーを実行するために /updates ディレクトリーに移動し、以下のコマンドを入力します。

   ```
   sh installer.sh
   ```
9. システムを再始動してください。

第 2 章 QRadar Packet Capture クイック・リファレンス

パケットをキャプチャーするためには、IBM Security QRadar Packet Capture のネットワーク設定および接続設定を構成する必要があります。

Intel SFP+ と SFP の互換性リスト

QRadar Packet Capture アプライアンスには、キャプチャー・ポートが 1 つだけあります (DNA0)。QRadar Packet Capture アプライアンスには SFP トランシーバーが装備されていないので、SFP+ 10G または SFP 1G (Copper RJ45) のいずれかをキャプチャー・ポートに取り付ける必要があります。

QRadar Packet Capture アプライアンスの SFP モジュールを購入する場合は、以下のベンダーの Web サイトを参照してください。

- Digi-Key Web サイト (http://www.digikey.com)
- Mouser Electronics Web サイト (http://www.mouser.com)
- CDW Web サイト (http://www.cdw.com)
- Newegg Web サイト (https://www.newegg.com)
- Amazon web site (http://amazon.com)

SFP 1G を取り付ける場合、キャプチャー速度が 1 Gbps に制限されます。

複数の 1G 接続を持つために、10G アウトバウンド・ポートから QRadar Packet Capture SFP+ 10G ポートに入る場所の前に、スイッチまたはアグリゲーターを置くことができます。その結果、QRadar Packet Capture 10G SFP+ インターフェースに複数の 1Gb ポートを集約することができます。

以下のリストで、SFP+ モジュールと SFP モジュールの要件を説明します。

部品番号	説明
E10GSFPSR	Dual Rate 10GBASE-SR/1000BASE-SX、 Intel Ethernet SFP+ SR Optical
E10GSFPLR	Dual Rate 10GBASE-LR/1000BASE-LX、 Intel Ethernet SFP+ LR Optical
FCLF8522P2BTL	1000BASE-T、 Finisar Gigabit Ethernet Transceiver
453153-001	HP Gigabit SX Transceiver

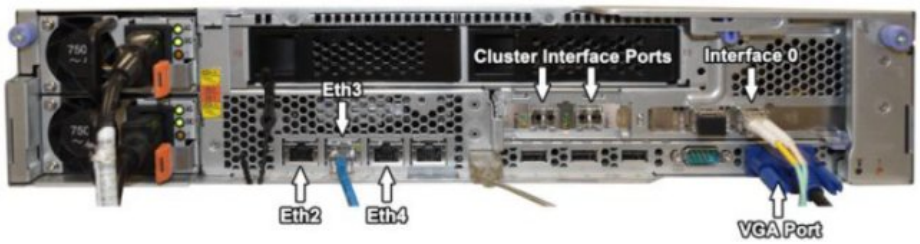
ネットワーク構成

ネットワークの初期構成を行うには、ディスプレイ、キーボード、およびオンボード・ポートへのイーサネット接続が必要です。デフォルトでは、システムにはアクティブな DHCP ポートがあります。

使用中のイーサネット・ポートの IP アドレスが判明している場合は、記録の開始に進みます。

1. サーバーに対して、リモート・アクセスのためのネットワーク接続を提供します。

   次の図に示すオンボード・イーサネット・ポート Eth2、Eth3、または Eth4 のいずれかへのイーサネット接続を提供します。



2. ネットワーク・キャプチャー用のネットワーク接続を提供します。

   次の図に示すインターフェース 0 ポートを使用することで、ファイバー 10G 接続を提供します。

   重要**:** 接続上にトラフィックが存在することを確認します。トラフィックをキャプチャーするには、Tap ポートまたは SPAN (ミラー) ポートを使用する必要があります。スイッチで SPAN ポートを使用している場合、スイッチで SPAN ポートに割り当てられている優先順位が低いと、一部のパケットがドロップされることがあります。

3. SSH およびポート 4477 を使用して、root ユーザーとしてログインします。

   デフォルトのユーザー名は `root` です。デフォルト・パスワードは、`P@ck3t08..` です。

4. IP アドレスを記録します。

   ログインした後、端末を開いて以下のコマンドを入力します。`#ifconfig -a`

   このコマンドにより、接続されているイーサネット・ポートの IP アドレスが表示されます。

   注**:** 静的 IP アドレスの設定については、「*IBM Security QRadar Packet Capture* ユーザーズ・ガイド」を参照してください。

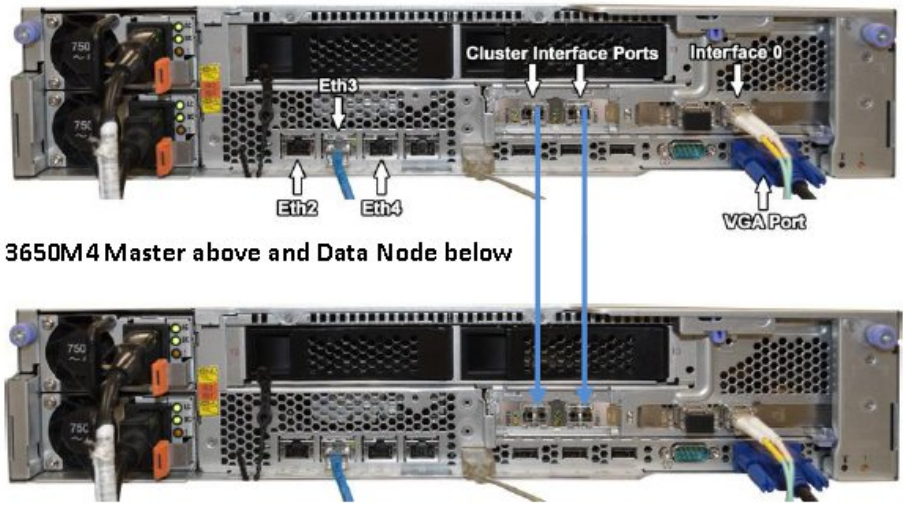
5. 接続をテストします。

   接続をテストするには、内部ネットワークを ping するか、ポート 4477 で SSH を使用してリモート・ログインします。先へ進む前に、必ず接続が正常であることを確認してください。

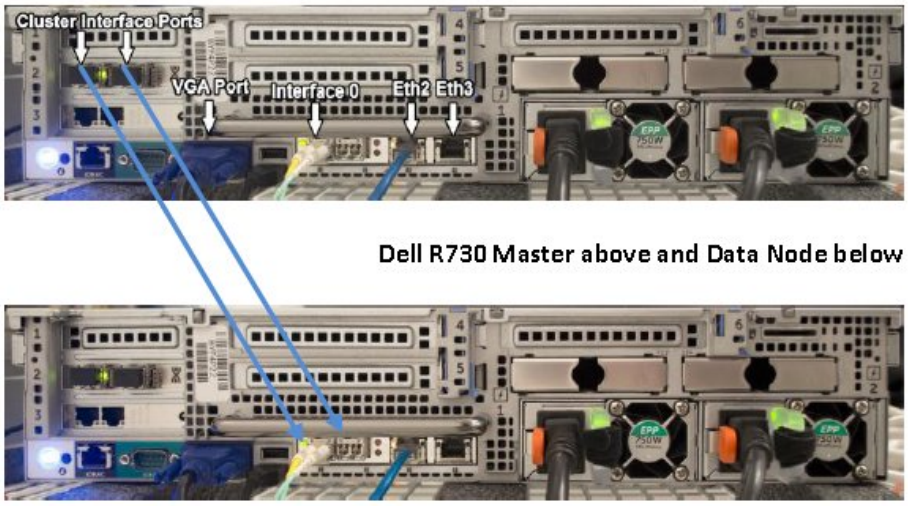
クラスターの接続

ネットワークをスタンドアロン・システムまたはマスター・システムに正常に接続したら、マスター・パケット・キャプチャー・アプライアンスを QRadar Packet Capture のデータ・ノード・アプライアンスに接続します。スタンドアロン・パケット・キャプチャー・システムのみがある場合、この手順は必要ありません。

1. ご使用のパケット・キャプチャー・デバイスのハードウェア図を参照してください。
   - IBM System x3650 M4 マスター・パケット・キャプチャー・デバイスと QRadar Packet Capture のデータ・ノードとの接続



   - Dell R730 パケット・キャプチャー・デバイスと QRadar Packet Capture のデータ・ノード



2. 上の図の矢印で示すように、パケット・キャプチャー・デバイスの背面で、マスターの左のクラスター・インターフェース・ポートを 1 つめのデータ・ノードの左のインターフェース・ポートに接続します。

3. 2 つめのデータ・ノードがある場合、マスターの右のクラスター・インターフェース・ポートを 2 つめのデータ・ノードの右のインターフェース・ポートに接続します。
4. マスター・システムの端末から、次のように ping テストを使用して接続を検査します。

   ```
   ping 1.1.1.2
   ping 2.2.2.2
   ```

5. ping からの応答を受信しない場合、データ・ノード・インターフェース側のケーブル接続のみを入れ替えます。
   - 1 つのデータ・ノードのみを接続した場合、正常な応答が必要な ping は 1 つのみです。
   - ケーブルを入れ替えても ping テストからの応答がない場合、データ・ノード NIC に接続したケーブルを 2 次的にインストールされている光イーサネット NIC (存在する場合) に切り替えて、ping テストを繰り返します。

記録の開始

システムに正常にネットワーク接続できるようになったら、ネットワーク・パケットのディスクへの記録およびネットワーク上のトラフィックに関する統計の表示を開始できます。

1. Web ブラウザーを開いて、以下のデバイスにアクセスします。

   `https://`*`PCAP_IP_Address`*`:41390`

2. 以下のユーザー情報を使用してログインします。

   ユーザー: `continuum`

   パスワード: `P@ck3t08..`

3. 物理的に接続した各データ・ノード (スレーブ) を有効にします。
4. 記録を開始します。

   ログインしてデータ・ノードを有効にしたら、「キャプチャー状態 **(Capture State)**」ページに移動し、「キャプチャーの開始 **(Start Capture)**」をクリックします。

   注**:** キャプチャーが開始されると、すべてのキャプチャーの詳細を含む統計ウィンドウが表示されます。

特記事項

本書は米国 IBM が提供する製品およびサービスについて作成したものです。

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

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

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

IBM およびその直接または間接の子会社は、本書を特定物として現存するままの状態で提供し、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任を負わないものとします。国または地域によっては、法律の強行規定により、保証責任の制限が禁じられる場合、強行規定の制限を受けるものとします。

この情報には、技術的に不適切な記述や誤植を含む場合があります。本書は定期的に見直され、必要な変更は本書の次版に組み込まれます。IBM は予告なしに、随時、この文書に記載されている製品またはプログラムに対して、改良または変更を行うことがあります。

本書において IBM 以外の Web サイトに言及している場合がありますが、便宜のため記載しただけであり、決してそれらの Web サイトを推奨するものではありません。それらの Web サイトにある資料は、この IBM 製品の資料の一部ではありません。それらの Web サイトは、お客様の責任でご使用ください。

IBM は、お客様が提供するいかなる情報も、お客様になんら義務も負わせない適切な方法で、使用もしくは配布することがあります。

本プログラムのライセンス保持者で、(i) 独自に作成したプログラムとその他のプログラム (本プログラムを含む) との間での情報交換、および (ii) 交換された情報の相互利用を可能にすることを目的として、本プログラムに関する情報を必要とする方は、下記に連絡してください。

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

本プログラムに関する上記の情報は、適切な使用条件の下で使用することができますが、有償の場合もあります。

本書で説明されているライセンス・プログラムまたはその他のライセンス資料は、IBM 所定のプログラム契約の契約条項、IBM プログラムのご使用条件、またはそれと同等の条項に基づいて、IBM より提供されます。

記載されている性能データとお客様事例は、例として示す目的でのみ提供されています。実際の結果は特定の構成や稼働条件によって異なります。

IBM 以外の製品に関する情報は、その製品の供給者、出版物、もしくはその他の公に利用可能なソースから入手したものです。IBM は、それらの製品のテストは行っておりません。したがって、他社製品に関する実行性、互換性、またはその他の要求については確証できません。IBM 以外の製品の性能に関する質問は、それらの製品の供給者にお願いします。

IBM の将来の方向性および指針に関する記述は、予告なく変更または撤回される場合があります。これらは目標および目的を提示するものにすぎません。

表示されている IBM の価格は IBM が小売り価格として提示しているもので、現行価格であり、通知なしに変更されるものです。卸価格は、異なる場合があります。

本書には、日常の業務処理で用いられるデータや報告書の例が含まれています。より具体性を与えるために、それらの例には、個人、企業、ブランド、あるいは製品などの名前が含まれている場合があります。これらの名称はすべて架空のものであり、名称や住所が類似する企業が実在しているとしても、それは偶然にすぎません。

商標

IBM、IBM ロゴおよび ibm.com® は、世界の多くの国で登録された International Business Machines Corporation の商標です。他の製品名およびサービス名等は、それぞれ IBM または各社の商標である場合があります。現時点での IBM の商標リストについては、http://www.ibm.com/legal/copytrade.shtml をご覧ください。

製品資料に関するご使用条件

これらの資料は、以下のご使用条件に同意していただける場合に限りご使用いただけます。

適用度

IBM Web サイトの「ご利用条件」に加えて、以下のご使用条件が適用されます。

個人使用

これらの資料は、すべての著作権表示その他の所有権表示をしていただくことを条件に、非商業的な個人による使用目的に限り複製することができます。ただし、IBM の明示的な承諾をえずに、これらの資料またはその一部について、二次的著作物を作成したり、配布 (頒布、送信を含む) または表示 (上映を含む) することはできません。

商業的使用

これらの資料は、すべての著作権表示その他の所有権表示をしていただくことを条件に、お客様の企業内に限り、複製、配布、および表示することができます。ただし、IBM の明示的な承諾をえずにこれらの資料の二次的著作物を作成したり、お客様の企業外で資料またはその一部を複製、配布、または表示することはできません。

権限

ここで明示的に許可されているもの以外に、資料や資料内に含まれる情報、データ、ソフトウェア、またはその他の知的所有権に対するいかなる許可、ライセンス、または権利を明示的にも黙示的にも付与するものではありません。

資料の使用が IBM の利益を損なうと判断された場合や、上記の条件が適切に守られていないと判断された場合、IBM はいつでも自らの判断により、ここで与えた許可を撤回できるものとさせていただきます。

お客様がこの情報をダウンロード、輸出、または再輸出する際には、米国のすべての輸出入 関連法規を含む、すべての関連法規を遵守するものとします。

IBM は、これらの資料の内容についていかなる保証もしません。これらの資料は、特定物として現存するままの状態で提供され、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任なしで提供されます。

IBM オンラインでのプライバシー・ステートメント

サービス・ソリューションとしてのソフトウェアも含めた IBM ソフトウェア製品 (「ソフトウェア・オファリング」) では、製品の使用に関する情報の収集、エンド・ユーザーの使用感の向上、エンド・ユーザーとの対話またはその他の目的のために、Cookie はじめさまざまなテクノロジーを使用することがあります。多くの場合、ソフトウェア・オファリングにより個人情報が収集されることはありません。IBM の「ソフトウェア・オファリング」の一部には、個人情報を収集できる機能を持つものがあります。ご使用の「ソフトウェア・オファリング」が、これらの Cookie およびそれに類するテクノロジーを通じてお客様による個人情報の収集を可能にする場合、以下の具体的事項を確認ください。

このソフトウェア・オファリングは、展開される構成に応じて、セッション管理および認証の目的のために、それぞれのお客様のセッション ID を、セッションごとの Cookie を使用して収集する場合があります。これらの Cookie は無効にできますが、その場合、これらを有効にした場合の機能を活用することはできません。

この「ソフトウェア・オファリング」が Cookie およびさまざまなテクノロジーを使用してエンド・ユーザーから個人を特定できる情報を収集する機能を提供する場合、 お客様は、このような情報を収集するにあたって適用される法律、ガイドライン等を遵守する必要があります。これには、エンドユーザーへの通知や同意の要求も含まれますがそれらには限られません。

このような目的での Cookie を含む様々なテクノロジーの使用の詳細については、IBM の『IBM オンラインでのプライバシー・ステートメント』(http://www.ibm.com/privacy/details/jp/ja/) の『クッキー、ウェブ・ビーコン、その他のテクノロジー』および『IBM Software Products and Software-as-a-Service Privacy Statement』(http://www.ibm.com/software/info/product-privacy) を参照してください。

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