IBM Security QRadar Incident Forensics
バージョン 7.2.8

IBM QRadar Network Packet Capture 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 V7.2.8 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 7.2.8
IBM QRadar Network Packet Capture
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 2016.

目次

© Copyright IBM Corp. 2016

QRadar Network Packet Capture のインストールの概要

本書は、IBM® QRadar® Network Packet Capture のインストールおよび構成に必要な情報を提供します。

対象読者

QRadar Network 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およびデバイスの構成に精通していなければなりません。

テクニカル・ドキュメント

IBM Security QRadar 製品ライブラリーで QRadar 製品資料を見つけるには、『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

© Copyright IBM Corp. 2016

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 Network Packet Capture をインストールするための前提条件

QRadar Network Packet Capture アプライアンスをインストールする前に、ご使用のシステムが最小ハードウェア要件を満たしていることを確認してください。

ハードウェアの最小要件を以下の表に示します。

表 1. QRadar Network Packet Capture をインストールするためのハードウェア要件

説明	**Lenovo**	**Dell**
CPU	E5-2680 v4 12C 2.5 GHz 30 MB 2133 MHz	E5-2660 v3 2.6 GHz 25 MB 2133 MHz
メモリー	128 GB	128 GB
RAID コントローラー	M1215 SAS/SATA	PERC H730P、2 GB キャッシュ
OS HDD	2 x 1 TB、7.2 K、12 Gbps、NL SAS 2.5"、G3HS RAID 1	2 x 1 TB、7.2K、12 Gbps、NL SAS 2.5"、RAID 1
CAP HDD	12 x 6 TB、7.2 K、12 Gbps、NL SAS 3.5"、G2HS 512e RAID 5	12 x 6 TB、7.2 K、12 Gbps、NL SAS 3.5"、512e RAID 5
ネットワーク・アクセラレーター	NT40E3-4	NT40E3-4

セットアップするには、アプライアンスに付属する USB キーからシステムを始動する必要があります。USB には IBM QRadar Network Packet Capture 用の .iso イメージ・ファイルが格納されています。

QRadar Network Packet Capture のインストール

アプライアンスに付属する USB キーを使用して QRadar Network Packet Capture アプライアンスをインストールします。

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。

- 管理者として QRadar Network Packet Capture アプライアンスにログインしている。
- システム要件を満たしている。
- 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。

© Copyright IBM Corp. 2016

このタスクについて

注**:** アプライアンスを再インストールすると、キャプチャーしたデータおよび QRadar Network Packet Capture の構成がすべて失われます。

手順

1. ISO に接続します。コマンド `mkdir /media/usb` を入力して `/media/usb` ディレクトリーを作成します。
2. コマンド `mount -o loop <QRadar_ISO> /media/usb` を入力して ISO イメージをマウントします。
3. マシンの電源を入れ、**F12** を押して Boot Manager に入ります。
4. 「**One Shot BIOS Boot**」を選択します。
5. 「**Disk connected to front USB2: xxxx**」を選択します。

   注**:** 「**One Shot BIOS Boot**」で「**USB2**」が使用可能な状態になっていない場合は、USB キーがブート可能デバイスとして認識されていません。QRadar Network Packet Capture アプライアンスを再始動すると、この問題が解決します。
   QRadar Network Packet Capture アプライアンスが再始動を完了し、USB キーからファクトリー・イメージをインストールします。
6. ファクトリー・イメージのインストールが完了した後でプロンプトが表示されたら、アプライアンスを再始動してください。

タスクの結果

ファクトリー・イメージが再インストールされました。QRadar Network Packet Capture アプライアンスを始動できます。QRadar Network Packet Capture で IP、DNS、ゲートウェイ、およびネットマスクを構成する必要があります。

第 2 章 QRadar Network Packet Capture 構成の要件

IBM QRadar Network Packet Capture をインストールした後は、本ソフトウェアを使用する前に必ず構成してください。例えば、ネットワーク設定の構成、ユーザー・アカウントのセットアップ、日時の同期、およびロケーション名と連絡先の詳細の構成を行う必要があります。

QRadar Network Packet Capture を構成する前に、以下の要件が満たされていることを確認してください。

- 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。
- IBM QRadar Network Packet Capture アプライアンスの電源がオンになっている。
- 管理者として QRadar Network Packet Capture にログインしている。

  デフォルトのユーザー名は `admin` であり、デフォルトのパスワードは `pandion` です。

IP アドレスおよびネットワーク設定の構成

デフォルトでは、IBM QRadar Network Packet Capture は動的ホスト構成プロトコル (DHCP) クライアントとして機能し、DHCP を使用して IP アドレスを割り振ります。DHCP リースを取得できない場合は、デフォルトの IP アドレス 192.168.100.100 を使用します。DHCP を使用することも、手動でネットワーク設定を構成することもできます。

始める前に

注**:** QRadar Network Packet Capture アプライアンスがグループのメンバーである場合は、ネットワーク構成の設定を変更しないでください。その場合は、いったんグループから登録抹消してからネットワーク構成を変更し、グループに再登録してください。DHCP からの QRadar Network Packet Capture デバイス IP アドレスおよびホストを割り当てる、完全な DHCP または DNS インフラストラクチャーを使用してください。

手順

1. QRadar Network Packet Capture コンソールでネットワーク設定を構成するには、以下の手順を使用します。
   a. 「ネットワークの構成 **(Configure network)**」をクリックして Enter キーを押します。
   b. 「**QRadar Network Packet Capture** の **IP** 設定 **(QRadar Network Packet Capture IP Settings)**」というプロンプトでネットワーク設定を構成します。
   c. DHCP を使用する場合は、U を押してから Enter キーを押します。
   d. DHCP を使用しない場合は、A を押してから Enter キーを押します。

© Copyright IBM Corp. 2016

2. 以下の手順を使用してネットワーク設定を構成します。
   a. 「管理」タブで「ネットワークの構成 **(Configure network)**」ウィジェットに移動し、IP アドレスまたは DHCP のオプションを構成します。
   b. 「適用」を選択して変更内容を保存します。

QRadar Network Packet Capture が稼働していることを検査する

QRadar Network Packet Capture を構成した後は、キャプチャー・ポート、時刻同期、およびアプライアンス背面のアクセラレーター LED を調べて、正しく機能していることを確認してください。

1. キャプチャー・ポートを確認するには、「ダッシュボード」タブの「アクセラレーター **(Accelerator)**」に各ポートのリンク状況が表示されていることを確認します。ポートがアクティブになっている場合は、ポートのリンク速度が表示されます。

   データ・キャプチャーが開始されていない場合でも、リンク状況およびシステムの正常性は表示されます。

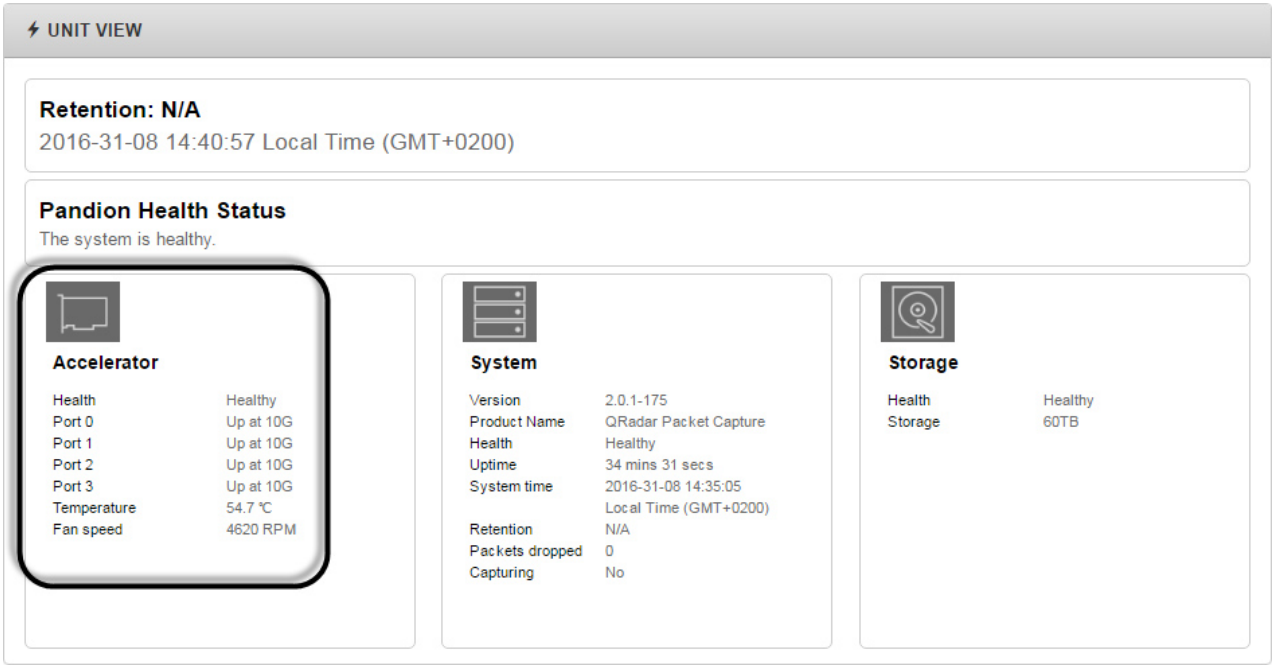

図 *1.* 「ユニット・ビュー *(UNIT VIEW)*」ウィジェット。

2. QRadar Network Packet Capture システムでキャプチャー・ネットワーク・インターフェース・カードの時刻同期のソースおよび状況を調べるには、「管理」タブ・メッセージの SYSLOGS メッセージを確認します。

   一般的なメッセージは、時刻同期ソースをいつ変更したかや、アクセラレーターが時刻ソースに対するロックをいつ取得または解放したかです。以下の構文は一般的な項目を表しています。

```
Adapter < number > time-sync status:
In-Sync: < Yes | No >
Current time-sync reference: < OsTime | PTP >
Skew (ns): < number >
Clock rate adjustment (ns): < number >
Clock Hard Reset: < Yes | No >
```

以下の例は一般的な項目を示しています。

```
Adapter 0 time-sync status:
In-Sync: Yes
Current time-sync reference: OsTime
Skew (ns): -1
Clock rate adjustment (ns): 503
Clock Hard Reset: No
```

PTP (Precision Time Protocol) マスターに対して同期している場合は、正確な状況についての詳細情報が PTP の項目に記録されます。アダプターが PTP モードの場合は、追加のログ項目に PTP 関連の情報が記録されます。以下の構文は PTP 項目を表しています。

```
Adapter < number > PTP time-sync status:
PTP Time: "--" | < PTP clock time > [ "(TAI)" ]
Port: < IPv4_address > | < IPv6_address > | "IEEE 802.3"
Link Status: < Down | 10M | 100M >
IPv4 Subnet Mask: < IPv4_address >
IPv4 Gateway: < IPv4_address >
DHCP Enabled: "Yes" | "No"
Profile Id: < six_times_2_hex digits >
Profile: < Default | Telecom | Power >
Clock Id: < six_times_2_hex digits >
Domain: < number > | "--"
VLAN: < number >
Delay Mechanism: "E2E", "P2P", "N/A"
PTP Filter: "Min", "PDV", "None", "N/A"
DelayAssemetry: < number >
Clock State: "Faulty" | "INACTIVE" | "SLAVE" | "--"
Mean Path Delay: <number>
GM Clock Identity: < 16_hex_digits >
```

以下の例は PTP 項目を示しています。

```
Adapter 0 time-sync status:
Adapter 0 PTP time-sync status:
PTP Time: Thu 26-May-2016 12:44:03.123456789 (TAI)
Port: 192.168.3.77
Link Status: 100M
IPv4 Subnet Mask: 192.168.3.0
IPv4 Gateway: 192.168.3.1
DHCP Enabled: Yes
Profile Id: 00:1b:19:00:01:00
Profile: Default
Clock Id: 00:0d:e9:03:a2:aa
Domain: 0
VLAN: 0
Delay Mechanism: E2E
PTP Filter: None
Delay Assemetry: 0
Clock State: SLAVE
Mean Path Delay: 0
GM Clock Identity: 000de9fffe03a2aa
```

パケット・キャプチャーの開始や停止

アプライアンスがキャプチャーするレコードの数を制御することができます。

手順

1. QRadar Network Packet Capture の「管理」タブをクリックします。
2. 「制御 (CONTROL)」ウィジェットに移動します。
3. 「トラフィックのキャプチャー **(Traffic Capture)**」を「オンにする **(Turn On)**」または「オフにする **(Turn Off)**」に設定します。

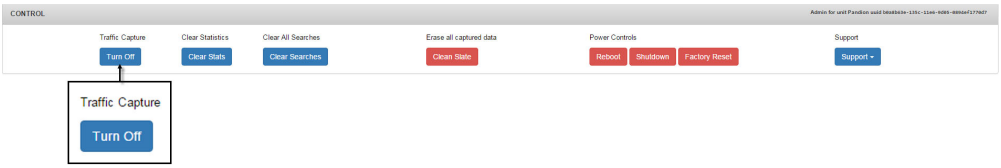

図 2. トラフィックのキャプチャー

デフォルトではパケット・キャプチャーがオンになっています。QRadar Network Packet Capture がパケットをキャプチャーしていない場合は、「トラフィックのキャプチャー **(Traffic Capture)**」が「オンにする **(Turn On)**」に設定されています。QRadar Network Packet Capture がパケットをキャプチャーしている場合は、「トラフィックのキャプチャー **(Traffic Capture)**」が「オフにする **(Turn Off)**」に設定されています。

特記事項

本書は米国 IBM が提供する製品およびサービスについて作成したものです。

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

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

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

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

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

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

IBM は、お客様が提供するいかなる情報も、お客様に対してなんら義務も負うことのない、自ら適切と信ずる方法で、使用もしくは配布することができるものとします。

© Copyright IBM Corp. 2016

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

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

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

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

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

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

IBM の将来の方向または意向に関する記述については、予告なしに変更または撤回される場合があり、単に目標を示しているものです。

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

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

商標

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

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