

IBM Security QRadar
バージョン 7.2.6

Packet Capture
ユーザーズ・ガイド

IBM

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、19 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
Version 7.2.6
Packet Capture Users 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

Packet Capture ユーザーズ・ガイドについて	v
第 1 章 QRadar Packet Capture V7.2.6 のユーザー用の新機能	1
第 2 章 QRadar Packet Capture の概要	3
第 3 章 QRadar Packet Capture のセットアップ	5
オペレーティング・システム・アカウントのパスワードの変更	6
QRadar Packet Capture サーバーの時刻と QRadar コンソールのシステム時刻との同期	7
第 4 章 キャプチャー使用の概要	9
第 5 章 データ・ノードの使用可能化	11
第 6 章 診断テストを目的とした時刻範囲内のパケットの検索	13
第 7 章 QRadar Packet Capture の問題のトラブルシューティング	15
特記事項	19
商標	20
プライバシー・ポリシーに関する考慮事項	21

Packet Capture ユーザーズ・ガイドについて

本書は、IBM® Security QRadar® 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。QRadar Packet Capture は IBM Security QRadar SIEM 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、Accessing 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の実践に関する注意事項

IT システムのセキュリティでは、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。ライセンスは、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 V7.2.6 のユーザー用の新機能

IBM Security QRadar Incident Forensics V7.2.6 では、パケット・キャプチャー取得の速度が向上し、データ収集とストレージを微調整するための事前キャプチャー・フィルターが導入されています。

個別のデータ・セグメントに素早く返される QRadar Packet Capture 検索結果

パケット・キャプチャー・データが個別のセグメントにダウンロードされるため、転送時間が短縮され、データをすぐに表示できます。データが小さいセグメントに分割されるため、検索されたデータに素早くアクセスできます。  詳細...

事前キャプチャー・パケット・フィルターを使用したデータ収集とストレージの微調整

キャプチャーする内容を定義して、ディスク・スペースを節減できます。パケット・キャプチャー・ストレージが制限されている場合は、リスクが最も高いと見なされるトラフィックのみをキャプチャーできます。ご使用のストレージ・リソースに合わせてパケット・キャプチャー収集機能を微調整できます。

第 2 章 QRadar Packet Capture の概要

IBM Security QRadar Packet Capture は、ネットワーク・トラフィックのキャプチャーおよび検索のアプリケーションです。

QRadar Packet Capture では、ライブ・ネットワーク・インターフェースから最大 10 Gbps の速度でネットワーク・パケットをキャプチャーし、パケット・ロスなくファイルに書き込むことができます。QRadar Packet Capture では、標準の PCAP ファイル・フォーマットを使用してネットワーク・トラフィックが格納されます。PCAP ファイル・フォーマットにより、既存のサード・パーティー分析ツールと容易に統合できます。

QRadar Packet Capture では、キャプチャーされたネットワーク・トラフィックを時刻およびパケット・エンベロープ・データで検索できます。アプライアンス・リソースを十分に確保し、検索を調整することで、検索とレコーダーのデータを同時に使用でき、データ損失も発生しません。また、ディスクへのパケットの記録も高性能です。

QRadar Packet Capture の機能

QRadar Packet Capture が提供する機能には以下のようなものがあります。

標準 PCAP ファイル・フォーマット

ネットワーク・トラフィックを保管するために使用されるファイル・フォーマットです。このファイル・フォーマットは、既存のサード・パーティー分析ツールと統合されます。

高性能なパケットのディスクへの記録

ライブ・ネットワークからのネットワーク・パケットをキャプチャーします。

マルチコアのサポート

QRadar Packet Capture は、マルチコア・アーキテクチャーでの使用を想定して設計されています。

直接 IO ディスク・アクセス

QRadar Packet Capture は、ディスクへの直接 IO アクセスを使用して、ディスク書き込みのスループットを最大化します。

リアルタイムの索引生成

QRadar Packet Capture では、パケット・キャプチャー中に自動的に索引を生成できます。この索引を BPF に似た構文を使用して照会し、指定した時間間隔の特定のパケットを素早く取得できます。

キャプチャー・データ容量を増大するためのクラスター

追加したストレージ容量に対して、データ・ノードでクラスターを作成することができます。

ダンプ・フォーマット

キャプチャー・ファイルは、マイクロ秒の解像度のタイム・スタンプとともに標準 PCAP フォーマットで保存されます。キャプチャー・ファイルは、ファイルのサイズに基づいて順番に保管されます。キャプチャー・ファイルはディレクトリーに格納されます。ディレクトリーの容量がいっぱいになると、キャプチャー・ファイルは事前構成された記録パラメーターに基づいて上書きされます。

キャプチャー速度

パケット・キャプチャー・アプライアンスでは、ネットワーク・トラフィックのキャプチャーの速度は、マスター・ノードに接続されたデータ・ノードがあるかどうかによって異なります。

- 接続されたデータ・ノードがないパケット・キャプチャー・アプライアンスでは、最大キャプチャー速度は 7 Gbps まで増加します。
- マスター・ノードに接続されたデータ・ノードがあるパケット・キャプチャー・アプライアンスでは、キャプチャー速度は 10 Gbps まで増加します。

関連概念:

9 ページの『第 4 章 キャプチャー使用の概要』

トラフィックをディスクにキャプチャーするには、キャプチャー・アプリケーションを開始します。レコーダー・コンポーネントによりトラフィック・データが事前構成されたディレクトリーに保存されます。ディレクトリーの容量がいっぱいになると、既存のファイルは上書きされます。

第 3 章 QRadar Packet Capture のセットアップ

IBM Security QRadar Packet Capture を使用する前に、いくつかの基本初期構成が必要です。

サポート対象の Web ブラウザー

以下の Web ブラウザーがサポートされています。

- Google Chrome
- Mozilla Firefox
- Microsoft Internet Explorer V10 以降

ネットワークのセットアップ

QRadar Packet Capture をリモート側で使用できるようにするには、イーサネット・ポート (通常は eth2、eth3、または eth4) のいずれかに IP アドレスを割り当てる必要があります。デフォルトでは、システムは DHCP を使用するように構成されています。ただし、初期構成では、VGA 互換モニターを接続し、システムをローカルに始動してログインし、ご使用のネットワークの静的 IP アドレスを構成することが必要になる場合があります。システムを始動したら、以下の資格情報を使用して root ユーザーとしてログインします。

```
username: root  
password: P@ck3t08..)
```

初期構成では、以下の手順を実行します。

1. VGA 互換モニターを接続します。
2. QRadar Packet Capture アプライアンスの電源をオンにします。
3. Linux オペレーティング・システムに root ユーザーとしてログオンします。

ユーザー名: root

パスワード: P@ck3t08..

デフォルト・パスワードを変更するには、6 ページの『オペレーティング・システム・アカウントのパスワードの変更』を参照してください。

4. ご使用のシステムが常に最新であるようにするために、IBM Fix Central (www.ibm.com/support/fixcentral/) で入手可能なソフトウェア・フィックスを適用します。
5. ご使用のネットワークの静的 IP アドレスを構成します。
 - a. MAC アドレスまたは eth2 インターフェースを取得するために、以下のコマンドを実行します。

```
ifconfig | grep eth2
```

eth0 インターフェースと eth1 インターフェースは使用できません。M4 xSeries のハードウェアには eth2 を使用します。

- b. MAC アドレスをメモします。
- c. /etc/sysconfig/network-scripts/ifcfg-eth2 ファイル内の設定を編集します。
 - 最初の行としてテキスト DEVICE=eth2 を追加します。
 - eth2 ポートの MAC アドレス HWADDR=xx:xx:xx:xx:xx のコメントを外します。
 - 設定 BOOTPROTO=static が構成されていることを確認します。
 - ご使用のネットワークに該当する情報を使用していることと、出力が以下の静的の例と同様になることを確認します。

```
DEVICE=eth2
#HWADDR=xx:xx:xx:xx:xx
BOOTPROTO="static"
BROADCAST="192.168.1.255"
DNS1="0.0.0.0"
DNS2="0.0.0.0"
GATEWAY="192.168.1.2"
IPADDR="192.168.1.1"
NETMASK="255.255.255.0"
NM_CONTROLLED="no"
ONBOOT="yes"
```

6. ファイルを保存します。
7. 設定を適用するために、以下のコマンドを実行します。

```
service network restart
```

8. 以下のコマンドを実行して、インターフェース設定を検証します。

```
ifconfig | more
```

DHCP の例: CentOS6.2 では、/etc/sysconfig/network-scripts/ifcfg-eth0 ファイルまたは /etc/sysconfig/network-scripts/ifcfg-eth1 ファイルの以下の設定を編集します。

```
BOOTPROTO="dhcp"
NM_CONTROLLED="no"
ONBOOT="yes"
```

リモート・ログイン

ローカル側に IP アドレスをセットアップすると、ポート 4477 で SSH を使用してリモート・ログオンすることで、アプライアンスを管理できます。

オペレーティング・システム・アカウントのパスワードの変更

アプライアンスをセットアップしたら、IBM Security QRadar Packet Capture 用のデフォルトのオペレーティング・システム・パスワードを変更します。

オペレーティング・システム・アカウントを変更するには、root ユーザーである必要があります。

QRadar Packet Capture のパスワードは、オペレーティング・システムのパスワードとは無関係です。adminusername および continuum のユーザー・アカウントは、初回ログイン時にパスワードを変更する必要があります。

手順

1. SSH を使用して、root ユーザーとしてログインします。

root ユーザーのデフォルト・パスワードは P@ck3t08.. です。

2. `continuum` および `root` のユーザー・アカウントのパスワードを変更するには、`passwd username` コマンドを使用します。

QRadar Packet Capture サーバーの時刻と QRadar コンソールのシステム時刻との同期

検索やデータに関連した機能を適切に実行できるように、IBM Security QRadar のデプロイメントで時刻設定の整合性を確保するには、すべてのアプライアンスを QRadar コンソール・アプライアンスと同期させる必要があります。管理者は、QRadar コンソール・アプライアンス上で `iptables` を更新してから、ポート 37 での `rdate` 通信を受け入れるように構成する必要があります。

始める前に

QRadar コンソールの IP アドレスまたはホスト名を知っていなければなりません。ホスト名は `nslookup` を使用して正しく解決されるものである必要があります。

デフォルトでは、QRadar Packet Capture デバイスのタイム・ゾーンは UTC (協定世界時) に設定されています。

手順

1. SSH を使用して、root ユーザーとして QRadar Packet Capture アプライアンスにログインします。
2. Network Time Protocol (NTP) サービスをオフにするには、コマンド `service ntpd stop` を入力します。
3. NTP のチェック構成をオフにするには、コマンド `chkconfig ntpd off` を入力します。
4. `crontab (crontable)` ファイルを編集して、同期を `cron` ジョブとしてスケジュールします。
 - a. コマンド `crontab -e` を入力します。
 - b. QRadar コンソールと 10 分ごとに同期するようにアプライアンスを構成するには、次のコマンドを入力します。`*/10 * * * * rdate -s Console_IP_Address`
Console_IP_Address 変数には IP アドレスまたはホスト名を使用します。
 - c. 構成変更を保存します。
 - d. 次のコマンドを入力して、`crond` の電源をオンにします。

```
service crond start
chkconfig crond on
```
5. QRadar コンソールで `iptables` を更新して QRadar Packet Capture デバイスからの `rdate` トラフィックを受け入れるようにします。
 - a. SSH を使用して、root ユーザーとして QRadar コンソール・アプライアンスにログインします。

b. /opt/qradar/conf/iptables.pre ファイルを編集します。

c. 次のコマンドを入力します。

```
-A QChain -m tcp -p tcp --dport 37 -j ACCEPT --src <PCAP_IP address>
```

複数の QRadar Packet Capture アプライアンスが存在する場合は、各 IP アドレスを 1 行で追加します。

例:

```
QChain -m tcp -p tcp --dport 37 -j ACCEPT --src 100.100.1.10  
QChain -m tcp -p tcp --dport 37 -j ACCEPT --src 100.100.1.11  
QChain -m tcp -p tcp --dport 37 -j ACCEPT --src 100.100.1.12
```

d. iptables.pre ファイルを保存します。

e. 次のコマンドを入力して、QRadar コンソールで iptables を更新します。

```
./opt/qradar/bin/iptables_update.pl
```

関連概念:

9 ページの『第 4 章 キャプチャー使用の概要』

トラフィックをディスクにキャプチャーするには、キャプチャー・アプリケーションを開始します。レコーダー・コンポーネントによりトラフィック・データが事前構成されたディレクトリーに保存されます。ディレクトリーの容量がいっぱいになると、既存のファイルは上書きされます。

第 4 章 キャプチャー使用の概要

トラフィックをディスクにキャプチャーするには、キャプチャー・アプリケーションを開始します。レコーダー・コンポーネントによりトラフィック・データが事前構成されたディレクトリーに保存されます。ディレクトリーの容量がいっぱいになると、既存のファイルは上書きされます。

トラブルシューティング: データが収集されない場合は、接続を介したトラフィックが存在することを確認してください。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。

始めに

システムをセットアップしたら、以下の手順を実行して、IBM Security QRadar Packet Capture にログインします。

1. Web ブラウザーを開き、デバイスの IP アドレスを入力します。
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..

デフォルトでは、「キャプチャー状態 (Capture State)」ページが表示されます。「**キャプチャーの開始 (Start Capture)**」または「**キャプチャーの停止 (Stop Capture)**」をクリックして記録を制御できます。

ヒント: ウィンドウの右上隅に製品バージョン番号が表示されます。

キャプチャー状態

「キャプチャー状態 (Capture State)」ページには以下の情報が表示されます。

- キャプチャーを実行中のインターフェース
- キャプチャー状況
- 開始/終了時刻
- システムでキャプチャーを実行した期間
- スループット・レート
- キャプチャーされたパケット数
- キャプチャーされたバイト数
- ドロップされたパケット数
- 使用可能なストレージ・スペース

クラスター構成では、使用可能なデータ・ノードごとにストレージの使用状況が表示されます。ネットワーク構成の問題または不適切な接続が原因で QRadar Packet Capture データ・ノードに到達できない場合は、ストレージ統計の代わりに次のメツ

セージが表示されます。「スレーブ・ノードは使用可能ですが、現在到達不可能です。(Slave node is enabled but is currently unreachable.)」

ネットワーク特性

ネットワークのスループットをグラフ形式で表示します。

ディスクへのキャプチャーの最大スループットはデフォルトでは 10 Gbps です。

キャプチャー履歴

実行済みまたは進行中のパケット・キャプチャーの履歴を表示します。

インライン圧縮

Forensics の調査をサポートするには、物理ディスクを追加せずに使用可能な仮想ストレージの容量を増やすことで、生のパケット・コンテンツをより長い期間保持することができます。新規のインライン圧縮オプションを使用して、QRadar Packet Capture アプライアンスにより大量のデータを保管できるようになりました。

圧縮量は、ペイロード内の圧縮されたビデオ・コンテンツの量に関連しています。例えば、5% 圧縮されたビデオがペイロードにある場合、13:1 で圧縮されます。「圧縮:ストレージ」率は、非圧縮サイズと圧縮サイズとの間の比率です。

表 1. インライン圧縮率

圧縮されたビデオ・ペイロードの割合 (%)	圧縮:ストレージの増幅率
0	17:1
5	13:1
10	6:1
20	4:1
40	2.4:1

関連概念:

3 ページの『第 2 章 QRadar Packet Capture の概要』

IBM Security QRadar Packet Capture は、ネットワーク・トラフィックのキャプチャーおよび検索のアプリケーションです。

関連タスク:

7 ページの『QRadar Packet Capture サーバーの時刻と QRadar コンソールのシステム時刻との同期』

検索やデータに関連した機能を適切に実行できるように、IBM Security QRadar のデプロイメントで時刻設定の整合性を確保するには、すべてのアプライアンスを QRadar コンソール・アプライアンスと同期させる必要があります。管理者は、QRadar コンソール・アプライアンス上で iptable を更新してから、ポート 37 での rdate 通信を受け入れるように構成する必要があります。

第 5 章 データ・ノードの使用可能化

マスター IBM Security QRadar Packet Capture デバイスを QRadar Packet Capture データ・ノードに物理的に接続した後で、QRadar Packet Capture データ・ノードを使用可能にする必要があります。QRadar Packet Capture データ・ノードを使用可能にすると、追加したストレージ容量に対してクラスターが作成されます。

アプライアンスの接続について詳しくは、「*QRadar Packet Capture Quick Reference Guide*」を参照してください。

制約事項: QRadar Packet Capture データ・ノードを使用不可にすると、Forensics Recovery でそのノード上のキャプチャー済みデータにアクセスできなくなります。

手順

1. 「ダッシュボード」タブで、トラフィック・キャプチャーを開始してから停止します。
2. 「クラスター」タブで、各データ・ノードについて、「有効」を選択します。状況として「**接続済み (Connected)**」が表示されます。
3. キャプチャーを再開します。

QRadar Packet Capture データ・ノードが使用可能になっています。QRadar Packet Capture データ・ノードが接続済みで実行中である場合、クラスター内の QRadar Packet Capture データ・ノードの状況は、「**接続済み (connected)**」に変更されます。

データ・ノード 1 またはデータ・ノード 2 がライセンス交付を受けている場合、ライセンス列には、使用したライセンスに応じて、「**永続 (Permanent)**」または「**評価 (Evaluation)**」のいずれかが表示されます。

マスター・ノードがデータ・ノードに接続した後で、ダッシュボード上に表示される圧縮 (仮想) ストレージ・サイズには、接続されたデータ・ノードのストレージ・サイズが含まれます。

第 6 章 診断テストを目的とした時刻範囲内のパケットの検索

キャプチャー時に作成される索引データを使用して、指定した時刻範囲と一致するパケットおよびパケット・メタデータ情報を含むパケット・キャプチャー (pcap) ファイルが生成されます。

制約事項: これらの検索は、診断のみを目的としています。抽出パーティションがいっぱいにならないようにするために、手動でのクリーンアップが必要です。

手順

1. 「検索」ページをクリックします。

デフォルト値があらかじめ入力されています。

2. 検索するキャプチャー済みトラフィックのインターフェースを選択します。

インターフェース構成が 1 つしかない場合は、それが自動的に選択されます。

3. 検索する時刻範囲の開始と終了の値を指定するか、またはデフォルトを変更します。
4. Berkeley Packet Filter (BPF) を指定します。

BPF の構文を使用して BPF フィルターを指定します。1 つの式が 1 つ以上のプリミティブで構成されます。複雑なフィルター式は、AND、OR、NOT の演算子を使用して作成されます。

プリミティブ・フィルターの例を以下に示します。

```
ether host 00:11:22:33:44:55
ether src host 00:11:22:33:44:55
```

```
ip host 192.168.0.1
ip dst host 192.168.0.1
```

```
ip6 host 2001:0db8:85a3:0042:0000:8a2e:0371:7334
ip6 src host 2001:0db8:85a3:0042:0000:8a2e:0371:7334
```

```
ip net 192.168.1.0/24
ip src net 192.168.1
```

```
port 80
udp port 9000
tcp src port 80
```

複雑なフィルターの例を以下に示します。

```
ip host 192.168.1.1 and 192.168.1.2
ip src 192.168.1.1 and dst 192.168.1.2
ip host 192.168.1.1 and tcp port (80 or 443)
(ip host 192.168.1.1 or 192.168.1.2) and (port 80 or 443)
```

5. 抽出するパケットの数を指定します。

抽出するパケット数の最大値のデフォルトは 10,000 です。この数値を 0 に変更すると、タイムラインとフィルターに一致するすべてのパケットが抽出されます。

6. 「**検索の開始 (Start Search)**」をクリックします。
7. 検索ページの「**アクション**」列に表示されているように、検索要求は小さいデータ・セグメントに分割されているため、検索要求全体がまだ実行中であってもデータにアクセスできます。PCAP ファイル番号を指定してから、「**PCAP ファイルのダウンロード**」ボタンをクリックして、検索を要求できます。

データ・セグメントのサイズは 128 MB ですが、最後のデータ・セグメントのサイズは可変です。

8. 検索キューの状態を確認するには、「**検索要求キュー (Search request queue)**」を参照します。
9. すべての完了した検索の履歴を確認するには、「**要求ログ (Request log)**」を参照します。
10. 手動検索をクリーンアップして、Forensics Recovery プロセス用のスペースが十分に確保されるようにします。
 - a. root としてログインします。

```
username: root
```

```
パスワード: P@ck3t08..
```

- b. 以下のコマンドを実行します。

```
rm -r /extraction/<name_of_search>
```

<name_of_search> 変数は、「完了した検索 (Completed Searches)」ページの名前列です。

第 7 章 QRadar Packet Capture の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、問題解決のための体系に基づくアプローチです。トラブルシューティングの目標は、何かが予期したとおりに動作しない理由を判別し、問題の解決方法を説明することです。

QRadar Packet Capture ソフトウェアの最新バージョンがインストールされていますか？

ソフトウェアの最新リリース・バージョンに必ずアップグレードしてください。ソフトウェア更新を適用した直後、または何らかの新規インストールの後には、変更が適用されるようにシステムを再始動してください。クラスター構成では、マスター・ノード・システムとすべてのデータ・ノード・システムが両方とも同じバージョンにアップグレードされていることを必ず確認してください。

RAID コントローラーおよびハード・ディスクで推奨されるファームウェアを使用していますか？

3650 M4 RAID コントローラーおよびハード・ディスク上にインストールされたファームウェア・リビジョンに関連する信頼性またはパフォーマンスの問題が発生した場合は、ファームウェア・リビジョンの最小要件が満たされていることを確認してください。

- 3650 M4 では、M5200 RAID コントローラー・ファームウェア・リビジョン (2015 年 5 月 27 日のバージョン 24.7.0-0052 以降) が必要です。

Red Hat Linux コマンド・ラインから .bin ファイルを実行します。

- IBM Lenovo では、2015 年 5 月 15 日のリビジョン以降が必要です。

Red Hat Linux コマンド・ラインから .bin ファイルを実行します。

キャプチャー・ポートは正しく接続されていますか？

IBM Security QRadar Packet Capture デバイスがキャプチャーできるのは、インターフェース 0 のみです。

イーサネット・ネットワーク接続は正しく構成されていますか？

イーサネット・インターフェースが確実に IP アドレスに割り当てられるようにするには、接続されているインターフェースに対して `ifconfig` コマンドを実行します。

アドレスが構成されていない場合は、対応する `ifcfg-eth*` ファイルを編集して、アドレスを構成します。

- この DHCP の例では、`/etc/sysconfig/network-scripts/ifcfg-eth2` にある次の設定を編集して、`eth2` を該当する設定に置き換えます。

```
BOOTPROTO="dhcp"
NM_CONTROLLED="no"
ONBOOT="yes"
```

- この静的 IP アドレスの例では、`/etc/sysconfig/network-scripts/ifcfg-eth2`にある次の設定を編集して、`eth2` を該当する設定に置き換えます。

```
BOOTPROTO="static"
BROADCAST="192.168.1.255"
DNS1="0.0.0.0"
DNS2="0.0.0.0"
GATEWAY="192.168.1.2"
IPADDR="192.168.1.1"
NETMASK="255.255.255.0"
NM_CONTROLLED="no"
ONBOOT="yes"
```

設定を変更したら、`ifconfig` コマンドを実行して、ネットワーク・インターフェースを構成します。

システム時刻は正しく構成されていますか？

デフォルトでは、システム時刻は協定世界時 (UTC) に設定されていて、正しいシステム時刻を維持するために Network Time Protocol (NTP) およびパブリック・サーバーを使用するように構成されています。

システム・ハードウェア障害がありますか？

1. トラフィックが適切に生成されていて、ネットワーク・インターフェース・カード (NIC) によって受信されていることを確認してください。

インターフェース 0 接続のすぐ右にあるライトを確認してください。リンクを示す一番下のライトが、途切れずに点灯する必要があります。トラフィック・アクティビティを示す一番上のライトは、明滅している必要があります。

2. `/usr/local/nc/bin/dpdk_nic_bind.py -status` コマンドを実行します。

コマンドの結果は、次のような出力になる必要があります。

```
Network devices using DPDK-compatible driver
=====
0000:0f:00.0 '82599ES 10-Gigabit SFI/SFP+ Network Connection' drv=igb_uio
unused=ixgbe
0000:0f:00.1 '82599ES 10-Gigabit SFI/SFP+ Network Connection' drv=igb_uio
unused=ixgbe
Network devices using kernel driver
=====
0000:07:00.0 'I350 Gigabit Network Connection' if=eth2 drv=igb unused=igb_uio
*Active*
0000:07:00.1 'I350 Gigabit Network Connection' if=eth3 drv=igb unused=igb_uio
0000:07:00.2 'I350 Gigabit Network Connection' if=eth4 drv=igb unused=igb_uio
Other network devices
=====
<none>
```

システムはトラフィックをキャプチャーしていますか？

キャプチャー・セッションの開始後、システムがトラフィックをキャプチャーしているかどうかを確認するには、次のいずれかの方法を使用します。

- インターフェース 0 接続のすぐ右にあるライトを確認してください。トラフィック・アクティビティを示す一番上のライトは、明滅している必要があります。

- 「ネットワーク特性」ページで、グラフィカルな出力を確認します。
- コマンド・ラインで、`du -h /storage0/int0` コマンドを実行します。

結果は、次のような出力になります。

```
4.4G /storage0/int0/1_0
4.9G /storage0/int0/2_0
6.4G /storage0/int0/3_0
4.9G /storage0/int0/4_0
4.9G /storage0/int0/5_0
4.9G /storage0/int0/6_0
.
.
.
1.4T /storage0/int0/
```

このコマンドを繰り返し実行すると、返されるサブディレクトリーの数および割り振り量が増加します。

REST インターフェースは動作していますか？

`continuum` のユーザーの正しい (デフォルトではない) パスワードでパスワード部分を置き換えて、次のコマンドを実行します。

```
curl -k -v -X POST -G -d "username=continuum&password=password&action=ping" https://localhost/rest/forensics_fetch.php
```

結果は、次のような出力になります。

```
About to connect() to localhost port 443 (#0)
* Trying ::1... connected
* Connected to localhost (::1) port 443 (#0)
* Initializing NSS with certpath: sql:/etc/pki/nssdb
* warning: ignoring value of ssl.verifyhost
* skipping SSL peer certificate verification
* SSL connection using TLS_DHE_RSA_WITH_AES_128_CBC_SHA
* Server certificate:
* subject: E=root@localhost.localdomain,CN=localhost.localdomain,
OU=SomeOrganizationalUnit,
O=SomeOrganization,L=SomeCity,ST=SomeState,C=--
* start date: Mar 27 17:10:01 2014 GMT
* expire date: Mar 27 17:10:01 2015 GMT
* common name: localhost.localdomain
* issuer: E=root@localhost.localdomain,CN=localhost.localdomain,
OU=SomeOrganizationalUnit,
O=SomeOrganization,L=SomeCity,ST=SomeState,C=--
> POST /rest/forensics_fetch.php?username=continuum&password=
test&action=ping HTTP/1.1
> User-Agent: curl/7.19.7 (x86_64-redhat-linux-gnu) libcurl/7.19.7 NSS/3.15.3
zlib/1.2.3 libidn/1.18 libssh2/1.4.2
> Host: localhost
> Accept: */*
>
< HTTP/1.1 200 OK
< Date: Mon, 13 Oct 2014 20:08:20 GMT
< Server: Apache/2.2.15 (Red Hat)
< X-Powered-By: PHP/5.3.3
< Set-Cookie: PHPSESSID=54cf36otmg899b6bau03lu6jh6; path=/
< Expires: Thu, 19 Nov 1981 08:52:00 GMT
< Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
< Pragma: no-cache
< Content-Length: 85
< Connection: close
< Content-Type: application/json
```

```
<
* Closing connection #0
{"status":"success","message":"QRadar Packet Capture (c), Version 7.2.4.209¥n"}
```

continuum ユーザー・パスワードをリセットする方法

QRadar Packet Capture のユーザー・インターフェースでは continuum ユーザー・パスワードを変更できません。パスワードを出荷時のデフォルト値にリセットするには、`reset_default.sh` スクリプトを使用する必要があります。ユーザーが次回ログインするときに、パスワードの変更を求めるプロンプトが出されます。

`reset_default.sh` スクリプトを実行するには、コマンド・ラインに `root` ユーザーとしてログインし、以下のコマンドを入力します。

```
sh /var/www/html/mysql/reset_default.sh continuum
```

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 の将来の方向性および指針に関するすべての記述は、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。

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。

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。