IBM Security QRadar Incident Forensics
Version 7.3.0

QRadar Packet Capture Quick Reference Guide

Note

Before you use this information and the product that it supports, read the information in “Notices” on page 7.

Product information

This document applies to IBM QRadar Security Intelligence Platform V7.3.0 and subsequent releases unless superseded by an updated version of this document.

Contents

About this Packet Capture quick reference guide

This documentation provides you with quick reference information that you need to install and configure IBM® QRadar® Packet Capture. QRadar Packet Capture is supported by IBM Security QRadar.

Intended audience

System administrators who are responsible for installing QRadar Packet Capture must be familiar with network security concepts and device configurations.

Technical documentation

To find IBM Security QRadar product documentation in the QRadar products library, see Accessing IBM Security Documentation Technical Note (www.ibm.com/support/docview.wss?rs=0&uid=swg21614644).

Contacting customer support

For information about contacting customer support, see the Support and Download Technical Note (http://www.ibm.com/support/docview.wss?uid=swg21616144).

Statement of good security practices

IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

Please Note:

Use of this Program may implicate various laws or regulations, including those related to privacy, data protection, employment, and electronic communications and storage. IBM Security QRadar may be used only for lawful purposes and in a lawful manner. Customer agrees to use this Program pursuant to, and assumes all responsibility for complying with, applicable laws, regulations and policies. Licensee represents that it will obtain or has obtained any consents, permissions, or licenses required to enable its lawful use of IBM Security QRadar.

Chapter 1. Upgrading QRadar Packet Capture

To upgrade from QRadar Packet Capture V7.2.8 to V7.3.0, install a cumulative software fix pack on a QRadar Packet Capture appliance. The software version that is installed on the appliance must be build 7.2.6.241 .

Procedure

1. Ensure that there isn't packet capture or search activities in progress.
2. Use SSH to log in to your system as `root` user.
3. Download the `7.3.0-QRadar-PCAP-build<build_number>.sfs` fix pack from IBM Fix Central (http://www.ibm.com/support/fixcentral/)
4. Copy the fix pack to the `/tmp` directory.

   If space in the `/tmp` directory is limited, copy the fix pack to another location that has sufficient space.
5. Create the `/updates` directory by typing the following command:

   ```
   mkdir -p /updates
   ```
6. Use the **`cd`** command to change to the directory where you copied the fix pack file.

   ```
   cd /tmp
   ```
7. To mount the fix pack file to the `/updates` directory, type the following command:

   ```
   mount -o loop -t squashfs 7.3.0-QRadar-PCAP-build<build_number>.sfs
   /updates
   ```
8. To run the installer for the fix pack, change the directory to the `/updates` directory and type the following command:

   ```
   sh installer.sh
   ```
9. Restart the system.

Chapter 2. QRadar Packet Capture quick reference

Before you can capture packets, you must configure IBM Security QRadar Packet Capture network and connection settings.

Intel SFP+ and SFP compatibility list

The QRadar Packet Capture appliance has only one capture port (DNA0). The QRadar Packet Capture appliance is not equipped with a SFP transceiver, so you must install either an SFP+ 10G or SFP 1G (Copper RJ45) into the capture port.

To purchase SFP modules for your QRadar Packet Capture appliance, see the following vendor websites:

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

When the SFP 1G is installed, it truncates the capture rate to 1 Gbps.

To have multiple 1G connections, you can put a switch or an aggregator in front of where the 10G outbound port goes into the QRadar Packet Capture SFP+ 10G port. As a result, you can have multiple 1Gb ports aggregated into the QRadar Packet Capture 10G SFP+ interface.

The following list describes the SFP+ and SFP module requirements:

Part Number	Description
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

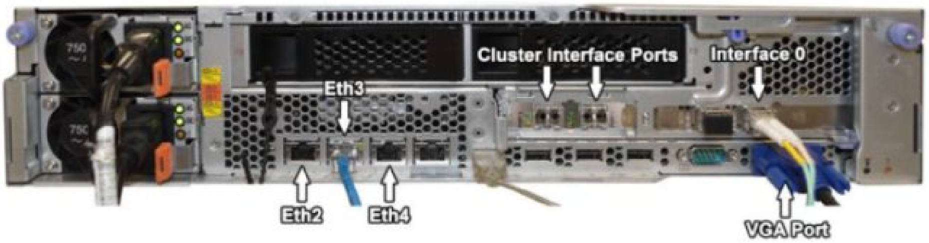
Network Configuration

To initially configure the network, a display, a keyboard, and an Ethernet connection to an onboard port are required. By default, the system has active DHCP ports.

If you know the IP address of the Ethernet port that is in use, go to Start recording.

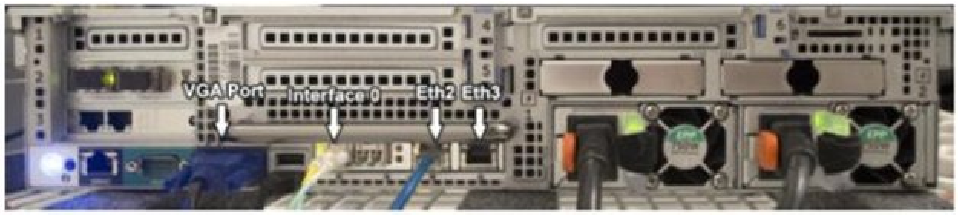
1. Provide a network connection for remote access to the server.

Provide an Ethernet connection to one of the onboard Ethernet ports, eth2, eth3, or eth4, as shown in the following diagram.



2. Provide a network connection for network capture.

   Provide fiber 10G connections by using the Interface 0 ports that are shown in the following diagram.



   Important: Ensure that there is traffic over the connections. To capture traffic, you must use a Tap or SPAN (mirror) port. When you use a SPAN port on a switch, if the switch assigns a lower priority to the SPAN port, some packets might be dropped.

3. Use SSH and port 4477 to log in as the root user.

   The default user name is: `root`. The default password is: `P@ck3t08.`.

4. Record the IP address.

   After you log in, open a terminal and enter the following command: `#ifconfig -a`

   This command provides the IP address of the Ethernet port that is connected.

   Note: For information about setting a static IP address, see the *IBM Security QRadar Packet Capture User Guide.*

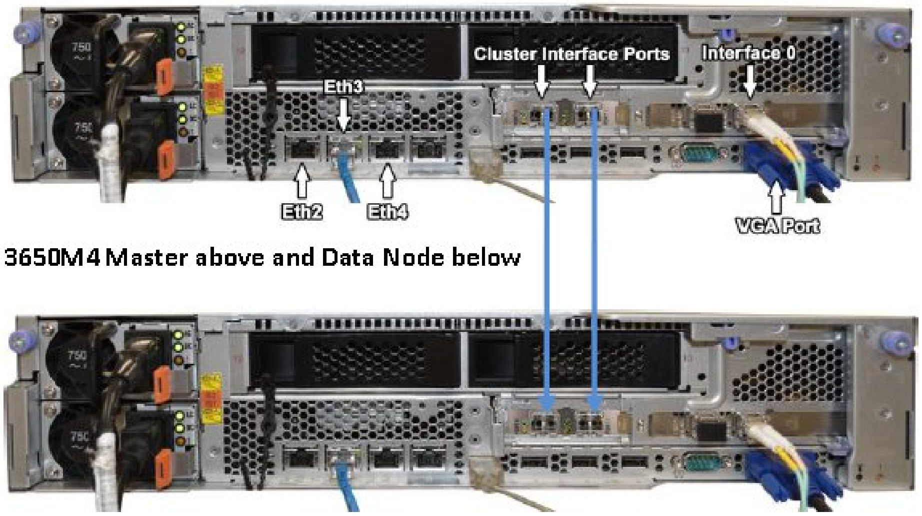
5. Test the connection.

   To test the connection, ping your internal network or log in remotely by using SSH on port 4477. Ensure that there is a successful connection before you continue.

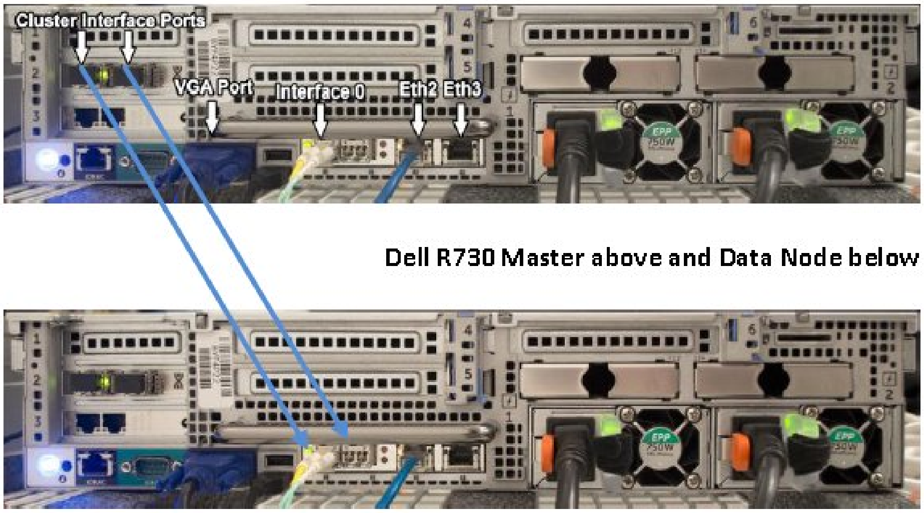
Connect the cluster

After you successfully connect the network to the standalone or master system, connect the master packet capture appliance to the QRadar Packet Capture Data Node appliances. If you have only a standalone packet capture system, this step is not required.

1. Refer to the hardware diagram for your packet capture device.
   - IBM System x3650 M4 master packet capture device and QRadar Packet Capture Data Node connection



- Dell R730 packet capture device and QRadar Packet Capture Data Node



2. On the back of the packet capture device, connect the left cluster interface port on the master to the left cluster interface port on the first data node, as indicated by the arrows in the preceding diagrams.
3. If there is a second data node, connect the right cluster interface port on the master to the right interface port on the second data node.
4. From a terminal on the master system, check the connections with a ping test:

   ```
   ping 1.1.1.2
   ping 2.2.2.2
   ```

5. If you do not receive a response from the ping, swap the cable connections on only the data node interfaces.
   - If only one data node is attached, only one ping must respond successfully.
   - If after you switch the cables and there is still no response from the ping test, switch the cables on the data node NIC to the second installed optical Ethernet NIC (if there is one) and repeat the ping test.

Start recording

After there is a successful network connection to the system, you can begin recording network packets to disk and viewing statistics about traffic on a network.

1. Open a web browser and access the device:

   `https://PCAP_IP_Address:41390`

2. Log in by using following user information:

   User: `continuum`

   Password: `P@ck3t08..`

3. Enable each data node (slave) that you physically connected.
4. Start recording.

   After you log in, and enabled any data nodes, go to the **Capture State** page and click **Start Capture**.

   Note: After the capture starts, a statistics window that contains all capture details is displayed.

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 U.S.A.

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you provide in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

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

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions..

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to actual people or business enterprises is entirely coincidental.

Trademarks

IBM, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.

Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability

These terms and conditions are in addition to any terms of use for the IBM website.

Personal use

You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of IBM.

Commercial use

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Rights

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

IBM Online Privacy Statement

IBM Software products, including software as a service solutions, (“Software Offerings”) may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering’s use of cookies is set forth below.

Depending upon the configurations deployed, this Software Offering may use session cookies that collect each user’s session id for purposes of session management and authentication. These cookies can be disabled, but disabling them will also eliminate the functionality they enable.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, See IBM's Privacy Policy at http://www.ibm.com/privacy and IBM's Online Privacy Statement at http://www.ibm.com/privacy/details the section entitled "Cookies, Web Beacons and Other Technologies" and the "IBM Software Products and Software-as-a-Service Privacy Statement" at http://www.ibm.com/software/info/product-privacy.

Printed in USA