IBM Security QRadar
Version 7.1.0 (MR1)

Using IPv6 with QRadar Technical Note

Note: Before using this information and the product that it supports, read the information in Notices and Trademarks on page 7.

© Copyright IBM Corp. 2012, 2013 All Rights Reserved US Government Restricted Rights - Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

CONTENTS

1 DEPLOYING QRADAR SIEM IN AN IPV6 ENVIRONMENT

Understanding IPv6 3
IPv6 Integration with QRadar SIEM 3
Network Activity Tab 3
Log Activity Tab 4
Searching, Grouping, and Reporting on IPv6 Fields 4
Custom Rules 4
Deployment Editor 4
IPv6 Configuration Considerations 4
Known Limitations 5

A NOTICES AND TRADEMARKS

Notices 7
Trademarks 9

1 DEPLOYING QRADAR SIEM IN AN IPV6 ENVIRONMENT

IPv4 and IPv6 addressing is supported for network connectivity and management of IBM Security QRadar SIEM software and appliances. When you install QRadar SIEM, you are prompted to specify whether your Internet protocol is an IPv4 or IPv6 environment.

Unless otherwise noted, all references to QRadar SIEM refer to QRadar SIEM, IBM Security QRadar Log Manager, and IBM Security QRadar Network Anomaly Detection.

This document includes the following topics:

- **Understanding IPv6**
- **IPv6 Integration with QRadar SIEM**
- **IPv6 Configuration Considerations**
- **Known Limitations**

Understanding IPv6

IPv6 is an Internet protocol for packet-switched networks. IPv6 has a larger address space than IPv4, thus allowing flexibility in allocating addresses and routing traffic. Event and flow records contain normalized fields for IPv6 addresses. Also, Device Support Modules (DSMs) can parse IPv6 source and destination address from event payloads.

IPv6 Integration with QRadar SIEM

The following QRadar SIEM components support IPv6:

- **Network Activity Tab**
- **Log Activity Tab**
- **Searching, Grouping, and Reporting on IPv6 Fields**
- **Custom Rules**
- **Deployment Editor**

Network Activity Tab

Depending on your deployment, the **Network Activity** tab can display four IP address fields:

- Source IP Address

- Destination IP Address
- IPv6 Source Address
- IPv6 Destination Address

To save space and indexing in a native IPv4 or IPv6 source environment, additional IP address fields are not stored or displayed. In a mixed IPv4/IPv6 environment, a flow record contains both IPv4 and IPv6 addresses.

IPv6 addresses are supported for both packet data, including sFlow, and NetFlow V9 data. However, older versions of NetFlow may not support IPv6.

Log Activity Tab

Depending on your deployment, the **Log Activity** tab can display four IP address fields:

- Source IP Address
- Destination IP Address
- IPv6 Source Address
- IPv6 Destination Address

When an address does not exist, template-based records are used to avoid wasted space.

DSMs can parse IPv6 addresses from the event payload. If any DSM can not parse IPv6 addresses, a log source extension can parse the addresses. For more information about log source extensions, see the *Log Sources Users Guide*.

Searching, Grouping, and Reporting on IPv6 Fields

In an IPv6 or mixed deployment, you can:

- Search events and flows using IPv6 parameters in the search criteria.
- Group and sort event and flow records based on IPv6 parameters.
- Base reports on data from IPv6-based searches.

Custom Rules

A custom rule has been added to support IPv6 addressing:

- SRC/DST IP = IPv6 Address
- IPv6-based building blocks have also been added for use in additional rules.

Deployment Editor

The deployment editor supports IPv6 addresses.

IPv6 Configuration Considerations

When deploying QRadar SIEM in an IPv6 or mixed environment, consider the following:

- To log in to QRadar SIEM in an IPv6 or mixed environment, the IP address must be wrapped in square brackets as follows:

  `https://[<IP Address>]`

Where **<IP Address>** is the IP address of the QRadar SIEM system.

- Both IPv4 and IPv6 environments can use a hosts file for address translation. An IPv6 or mixed environment Console requires that the client resolves the Console address by its host name. We recommend that you add the IP address of the IPv6 console to the /etc/hosts file on the client.
- Flow sources, such as NetFlow and sFlow, can be accepted from IPv4 and IPv6 addresses.
- Event sources, such as syslog and SNMP, can be accepted from IPv4 and IPv6 addresses.
- Disable superflows and flow bundling in an IPv6 environment. See the *IBM Security QRadar SIEM Administration Guide.*
- By default, QRadar SIEM currently does not support adding an IPv4-only managed host to an IPv6/IPv4 mixed mode console.

To setup an IPv4-only managed host in a mixed mode system:

Step 1 Install your QRadar SIEM Console as IPv6.

Step 2 On the Console, type the following command:

```
/opt/qradar/bin/setup_v6v4_console.sh
```

Step 3 To add an ipv4 managed host, type the following command

```
/opt/qradar/bin/add_v6v4_host.sh
```

Step 4 Add the managed host through the interface.

Known Limitations

When QRadar SIEM is deployed in an IPv6 environment, the following limitations are known:

- The network hierarchy is not updated to support IPv6. Some aspects of the QRadar SIEM deployment, including surveillance, searching, and analysis, do not take advantage of the network hierarchy. For example, within the **Log Activity** tab, you cannot search or aggregate events By Network.
- No IPv6-based asset profiles. Asset profiles are only created if QRadar SIEM receives events, flows, and vulnerability data for IPv4 hosts.
- No host profile test in custom rules for IPv6 addresses.
- No specialized indexing or optimization of IPv6 addresses.
- No IPv6-based sources and destinations for offenses.

A NOTICES AND TRADEMARKS

What's in this appendix:

- **Notices**
- **Trademarks**

This section describes some important notices, trademarks, and compliance information.

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

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

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 states 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 Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply 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 Corporation
170 Tracer Lane,
Waltham MA 02451, USA

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.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

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.

All 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 the names and addresses used by an actual business enterprise is entirely coincidental.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

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 *http:\\www.ibm.com/legal/copytrade.shtml*.