IBM Security QRadar
Version 7.1.0 (MR1)

QRadar Common Ports List Technical Note

Note: Before using this information and the product that it supports, read the information in Notices and Trademarks on page 11.

CONTENTS

1 QRadar SIEM Common Ports

This technical note provides a list of common ports used by QRadar SIEM, services, and components. The information provided in this document contains the assigned port number, descriptions, protocols, and the signaling direction for the port.

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:

QRadar SIEM Common Ports

The following table provides the listening ports for QRadar SIEM. The ports listed in this table are valid only when iptables is enabled on your QRadar SIEM system.

Table 1-1 Listening Ports Used by QRadar SIEM, Services, and Components

Port	Description	Protocol	Direction	Required for
22	SSH	TCP	QRadar SIEM Console to all other components	• Remote management access • Adding a remote system as a managed host • Log source protocols to retrieve files from external devices, for example the Log File protocol • End-users who use the command line to communicate from desktops to the QRadar SIEM Console • High Availability (HA) communication

Table 1-1 Listening Ports Used by QRadar SIEM, Services, and Components (continued)

Port	Description	Protocol	Direction	Required for
25	SMTP	TCP	From all managed hosts to your SMTP gateway	• Allowing QRadar SIEM to send e-mails to an SMTP gateway • Error and warning e-mail message delivery to an administrative email contact
37	Rdate (time)	UDP/TCP	• All systems to the QRadar SIEM Console • QRadar SIEM Console to the NTP or RDATE server	Time synchronization between the QRadar SIEM Console and managed hosts
80	Apache/https	TCP	• End users to the QRadar SIEM Console • End users to the QRadar Deployment Editor	• Communication and downloads from the QRadar Console to end-user desktops • Allowing the deployment editor application to download from the QRadar SIEM Console to end-user desktops
111	Port mapper	TCP/UDP	• QRadar SIEM managed hosts connecting to the QRadar SIEM Console. • End users connecting to the QRadar SIEM Console	Remote Procedure Calls (RPC) for required services, such as Network File System (NFS)
135 and dynamically allocated ports above 1024 for RPC calls.	DCOM	TCP	From Windows host providing events using Windows Management Instrumentation (WMI) to QRadar SIEM Consoles or Event Collectors	DCOM communication and the collection of Windows events using WMI. Firewalls between QRadar SIEM and the target Microsoft Windows host must be configured to allow DCOM communication. ***Note:*** *DCOM typically uses a range of random ports, which can be configured to use a specific range. For more information, see your Microsoft Windows documentation.*
161	SNMP agent	UDP	• QRadar SIEM managed hosts connecting to the QRadar SIEM Console • External log sources to QRadar SIEM Event Collectors	UDP listening port for the SNMP agent

Table 1-1 Listening Ports Used by QRadar SIEM, Services, and Components (continued)

Port	Description	Protocol	Direction	Required for
199	NetSNMP	TCP	• QRadar SIEM managed hosts connecting to the QRadar SIEM Console • External log sources to QRadar SIEM Event Collectors	TCP port for the NetSNMP daemon listening for communications (v1, v2c, and v3) from external log sources
443	Apache/https	TCP	• QRadar SIEM managed hosts connecting to the QRadar SIEM Console • End users connecting to the QRadar SIEM Console	• Configuration downloads to managed hosts from the QRadar SIEM Console • End users to have log in access to QRadar SIEM
514	Syslog	UDP	External log sources to QRadar SIEM Event Collectors	External log sources to send event data to QRadar SIEM components
762	Network File System mount daemon (mountd)	TCP/UDP	Connections between the QRadar SIEM Console and NFS server	The Network File System (NFS) mount daemon, which processes requests to mount a file system at a specified location
1514	Syslog-ng	TCP/UDP	Connection between the local Event Collector component and local Event Processor component to the syslog-ng daemon for logging	Internal logging port for syslog-ng
2049	NFS	TCP	Connections between the QRadar SIEM Console and NFS server	The Network File System (NFS) protocol to share files or data between components
2055	NetFlow data	UDP	From the management interface on the flow source (typically a router) to the QFlow Collector	NetFlow datagram from components, such as routers
4333	Redirect port	TCP		This port is assigned as a redirect port for Address Resolution Protocol (ARP) requests in QRadar SIEM Offense Resolution
5432	Postgres	TCP	Communication for the managed host used to access the local database instance	When provisioning managed hosts using the **Admin** tab
6543	High Availability heartbeat	TCP/UDP	Bi-directional between the secondary host and primary host in an HA cluster	Heartbeat ping from a secondary host to a primary host in an HA cluster to detect hardware or network failure

Table 1-1 Listening Ports Used by QRadar SIEM, Services, and Components (continued)

Port	Description	Protocol	Direction	Required for
7676, 7677, and four randomly bound ports above 32000.	Messaging connections (IMQ)	TCP	Message queue communications between components on a managed host.	Message queue broker for communications between components on a managed host Ports 7676 and 7677 are static TCP ports and four additional connections are created on random ports. For more information on randomly bound ports, see **Viewing Random Port Associations**.
7777 to 7782, 7790, 7791	JMX server ports	TCP	Internal communications, these ports are not available externally	JMX server (Mbean) monitoring for ECS, hostcontext, Tomcat, VIS, reporting, ariel, and accumulator services. These ports are used by QRadar SIEM support.
7789	HA Distributed Replicated Block Device (DRBD)	TCP/UDP	Bi-directional between the secondary host and primary host in an HA cluster	Distributed Replicated Block Device (DRBD) used to keep discs synchronized between the primary and secondary hosts in HA configurations
7800	Apache Tomcat	TCP	From the Event Collector to the QRadar SIEM Console	Real-time (streaming) for events
7801	Apache Tomcat	TCP	From the Event Collector to the QRadar SIEM Console	Real-time (streaming) for flows
7803	Apache Tomcat	TCP	From the Event Collector to the QRadar SIEM Console	Anomaly Detection Engine listening port
8000	Event Collection Service (ECS)	TCP	From the Event Collector to the QRadar SIEM Console	Listening port for specific Event Collect Service (ECS) events
8005	Apache Tomcat	TCP	None	This is a local port not used by QRadar SIEM.
8009	Apache Tomcat	TCP	From the HTTP daemon (httpd) process to Tomcat	Tomcat connector, where the request is used and proxied for the web service
8080	Apache Tomcat	TCP	From the HTTP daemon (httpd) process to Tomcat	Tomcat connector, where the request is used and proxied for the web service.
9995	NetFlow data	UDP	From the management interface on the flow source (typically a router) to the QFlow Collector	NetFlow datagram from components, such as routers

Table 1-1 Listening Ports Used by QRadar SIEM, Services, and Components (continued)

Port	Description	Protocol	Direction	Required for
10000	QRadar SIEM Web-Based System Administration Interface	TCP/UDP	End-user desktop to all QRadar SIEM hosts	Server changes, such as root password and firewalls
23111	SOAP Webserver	TCP		SOAP Webserver listening port for the Event Collection Service (ECS)
23333	Emulex Fibre Channel	UDP	End-user desktop to QRadar SIEM hosts containing a Fibre Channel card	Emulex Fibre Channel HBAnywhere Remote Management service (elxmgmt)
32004	Normalized Event Forwarding	TCP	Bi-directional between QRadar SIEM components	Normalized event data communicated from an off-site source or between Event Collectors
32005	Data flow	TCP	Bi-directional between QRadar SIEM components	Data flow communication port between Event Collectors when located on separate managed hosts
32006	Ariel queries	TCP	Bi-directional between QRadar SIEM components	Communication port between the Ariel Proxy server and the Ariel Query server
32009	Identity data	TCP	Bi-directional between QRadar SIEM components	Identity data communicated between the passive Vulnerability Information Service (VIS) and the Event Collection Service (ECS)
32010	Flow source listening port	TCP	Bi-directional between QRadar SIEM components	Flow listening port to collect data from QFlow Collectors
32011	Ariel listening port	TCP	Bi-directional between QRadar SIEM components	Ariel listening port for database searches, progress information, and other associated commands
32000-33999	Data flow (flows, events, flow context)	TCP	Bi-directional between QRadar SIEM components	Data flows, such as events, flows, flow context, and event search queries

Table 1-1 Listening Ports Used by QRadar SIEM, Services, and Components (continued)

Port	Description	Protocol	Direction	Required for
40799	PCAP data	TCP	From Juniper Networks SRX Series appliances to QRadar SIEM	Collecting incoming packet capture (PCAP) data from Juniper Networks SRX Series appliances ***Note:*** *The packet capture on your device can use an alternate port to 40799. For more information on configuring packet capture, see your Juniper Networks SRX Series appliance documentation.*
ICMP	ICMP		Bi-directional between the secondary host and primary host in an HA cluster	Testing the network connection between the secondary host and primary host in an HA cluster using Internet Control Message Protocol (ICMP)

All the ports listed in **Table 1-1** can be tunneled, by encryption, through port 22 over SSH.

Viewing Random Port Associations

Several ports allocate additional random port numbers for application services, for example, Message Queues (IMQ). You can view additional port numbers using telnet to connect to the localhost and look up the port number.

NOTE

Random port associations are not static port numbers. If a service is restarted, the ports generated for a service are reallocated and the service is provided with a new set of port numbers.

To view randomly allocated ports, perform the following steps:

Step 1 Using SSH, log in to your QRadar SIEM Console, as the root user.

Login: **`root`**

Password: **`<password>`**

Step 2 Type the following command:

`telnet localhost 7676`

A list of associated ports to the IMQ messaging connection port is displayed.

```
[root@qradar ~]# telnet localhost 7676
Trying 127.0.0.1...
Connected to localhost.localdomain (127.0.0.1).
Escape character is '^]'.
101 imqbroker 4.4 Update 1
portmapper tcp PORTMAPPER 7676
```

```
[imqvarhome=/opt/sun/mq/var,imqhome=/opt/sun/mq,sessionid=1067]
cluster_discovery tcp CLUSTER_DISCOVERY 55076
jmxrmi rmi JMX 0
[url=service:jmx:rmi://qradar.q1labs.inc/stub/rO0ABXNyAC5qYXZh]
admin tcp ADMIN 50825
jms tcp NORMAL 7677
cluster tcp CLUSTER 41771
```

Step 3 If no information is displayed, press the Enter key to terminate the connection.

```
Connection closed by foreign host.
```

Searching for Ports on QRadar SIEM

Netstat is a command line tool used to determine which ports are in use on your QRadar SIEM Console or managed host. The netstat command allows you to view all listening and established ports on the system.

To use the netstat command, perform the following steps:

Step 1 Using SSH log in to your QRadar SIEM Console, as the root user.

Login: **root**

Password: **<password>**

Step 2 Type the following command:

netstat -nap

A list of all listening and established ports is displayed sorted by protocol.

```
tcp    0    0 0.0.0.0:37      0.0.0.0:*    LISTEN    10163/xinetd
tcp    0    0 0.0.0.0:23333   0.0.0.0:*    LISTEN    4615/elxhbamgrd
tcp    0    0 127.0.0.1:199   0.0.0.0:*    LISTEN    32116/snmpd
tcp    0    0 0.0.0.0:1514    0.0.0.0:*    LISTEN    15522/syslog-ng
```

Step 3 To search for specific information from the netstat port list, type the following command:

netstat -nap | grep <port>

Where **<port>** is the port number or search term for the netstat search.

For example:

- **netstat -nap | grep 199 -** Displays all ports matching 199.
- **netstat -nap | grep postgres -** Displays all postgres related ports.
- **netstat -nap | grep LISTEN** - Displays information on all listening ports.

NOTE For more information on using the netstat command, type **netstat ?** for a list of netstat options.

A NOTICES AND TRADEMARKS

What's in this appendix:

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*.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.