IBM Security QRadar
Version 7.1.0 MR2

Common Ports Guide

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

CONTENTS

1 QRadar common ports

This technical note provides a list of common ports that are used by QRadar SIEM, services, and components.

The information that is provided in this document contains the assigned port number, descriptions, protocols, and the signaling direction for the port. Unless otherwise noted, the ports that are listed apply to all IBM Security QRadar products and appliances.

QRadar common ports

The listen ports for QRadar as listed in the following table are valid only when IPtables is enabled on your QRadar system.

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

Table 1-1 Listening ports that are used by QRadar, services, and components

Port	Description	Protocol	Direction	Required for
22	SSH	TCP	Bidirectional from the QRadar Console to all other components. Managed hosts that use encryption can establish multiple bidirectional SSH sessions to communicate securely. These SSH sessions are initiated from the managed host to provide data to the host that needs the data in the deployment. For example, Event Processor appliances can initiate multiple SSH sessions to the QRadar Console for secure communication. This communication can include tunneled ports over SSH, such as https data for port 443 and Ariel query data for port 32006. QFlow Collectors that use encryption can initiate SSH sessions to Flow Processor appliances that require data.	• 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 • Users who use the command line to communicate from desktops to the QRadar Console • High Availability (HA) communication

Table 1-1 Listening ports that are used by QRadar, services, and components (continued)

Port	Description	Protocol	Direction	Required for
25	SMTP	TCP	From all managed hosts to your SMTP gateway	• QRadar to send emails to an SMTP gateway • Error and warning email message delivery to an administrative email contact
37	Rdate (time)	UDP/TCP	• All systems to the QRadar Console • QRadar Console to the NTP or RDATE server	Time synchronization between the QRadar Console and managed hosts
80	Apache/https	TCP	• Users that connect to the QRadar Console • Users to the QRadar Deployment Editor	• Communication and downloads from the QRadar Console to user desktops • The Deployment Editor application to download and display deployment information
111	Port mapper	TCP/UDP	• Managed hosts that communicate to the QRadar Console. • Users that connect to the QRadar 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	• Bidirectional traffic between WinCollect agents and Windows operating systems that are remotely polled for events. • Bidirectional traffic between QRadar Consoles or Event Collectors that use the Microsoft Security Event Log Protocol and Windows operating systems that are remotely polled for events. • Bidirectional traffic between Adaptive Log Exporter agents and Windows operating systems that are remotely polled for events.	This traffic is generated by the following log source protocols: • WinCollect • Microsoft Security Event Log Protocol • Adaptive Log Exporter ***Note:*** *DCOM typically allocates a random port range for communication. The random port values can be configured in Microsoft Windows products to use a specific port. For more information, see your Microsoft Windows documentation.* For information on the Microsoft API, see your Microsoft documentation.

Table 1-1 Listening ports that are used by QRadar, services, and components (continued)

Port	Description	Protocol	Direction	Required for
137	Windows NetBIOS name service	UDP	• Bidirectional traffic between WinCollect agents and Windows operating systems that are remotely polled for events. • Bidirectional traffic between QRadar Consoles or Event Collectors that use the Microsoft Security Event Log Protocol and Windows operating systems that are remotely polled for events. • Bidirectional traffic between Adaptive Log Exporter agents and Windows operating systems that are remotely polled for events.	This traffic is generated by the following log source protocols: • WinCollect • Microsoft Security Event Log Protocol • Adaptive Log Exporter For information on the Microsoft API, see your Microsoft documentation. For information on the Microsoft API, see your Microsoft documentation.
138	Windows NetBIOS datagram service	UDP	• Bidirectional traffic between WinCollect agents and Windows operating systems that are remotely polled for events. • Bidirectional traffic between QRadar Consoles or Event Collectors that use the Microsoft Security Event Log Protocol and Windows operating systems that are remotely polled for events. • Bidirectional traffic between Adaptive Log Exporter agents and Windows operating systems that are remotely polled for events.	This traffic is generated by the following log source protocols: • WinCollect • Microsoft Security Event Log Protocol • Adaptive Log Exporter For information on the Microsoft API, see your Microsoft documentation.
139	Windows NetBIOS session service	TCP	• Bidirectional traffic between WinCollect agents and Windows operating systems that are remotely polled for events. • Bidirectional traffic between QRadar Consoles or Event Collectors that use the Microsoft Security Event Log Protocol and Windows operating systems that are remotely polled for events. • Bidirectional traffic between Adaptive Log Exporter agents and Windows operating systems that are remotely polled for events.	This traffic is generated by the following log source protocols: • WinCollect • Microsoft Security Event Log Protocol • Adaptive Log Exporter For information on the Microsoft API, see your Microsoft documentation.

Table 1-1 Listening ports that are used by QRadar, services, and components (continued)

Port	Description	Protocol	Direction	Required for
161	SNMP agent	UDP	• QRadar managed hosts that connect to the QRadar Console • External log sources to QRadar Event Collectors	UDP listening port for the SNMP agent
199	NetSNMP	TCP	• QRadar managed hosts that connect to the QRadar Console • External log sources to QRadar Event Collectors	TCP port for the NetSNMP daemon listening for communications (v1, v2c, and v3) from external log sources
443	Apache/https	TCP	Bidirectional traffic for secure communications from all products to the QRadar Console.	• Configuration downloads to managed hosts from the QRadar Console • QRadar managed hosts that connect to the QRadar Console • Users to have log in access to QRadar SIEM • QRadar Consoles that manage and provide configuration updates WinCollect agents
445	Microsoft Directory Service	TCP	• Bidirectional traffic between WinCollect agents and Windows operating systems that are remotely polled for events. • Bidirectional traffic between QRadar Consoles or Event Collectors that use the Microsoft Security Event Log Protocol and Windows operating systems that are remotely polled for events. • Bidirectional traffic between Adaptive Log Exporter agents and Windows operating systems that are remotely polled for events	This traffic is generated by the following log source protocols: • WinCollect • Microsoft Security Event Log Protocol • Adaptive Log Exporter For information on the Microsoft API, see your Microsoft documentation.
514	Syslog	UDP/TCP	• External network appliances that provide TCP syslog events use bidirectional traffic. • External network appliances that provide UDP syslog events use uni-directional traffic.	External log sources to send event data to QRadar components Syslog traffic includes WinCollect agents and Adaptive Log Exporter agents capable of sending either UDP or TCP events to QRadar.

Table 1-1 Listening ports that are used by QRadar, services, and components (continued)

Port	Description	Protocol	Direction	Required for
762	Network File System mount daemon (mountd)	TCP/UDP	Connections between the QRadar 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 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 Offense Resolution
5432	Postgres	TCP	Communication for the managed host that is used to access the local database instance	Required for provisioning managed hosts from the **Admin** tab
6543	High Availability heartbeat	TCP/UDP	Bidirectional 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
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 extra connections are created on random ports. For more information about randomly bound ports, see **Viewing random port associations**.
7777 - 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 support.

Table 1-1 Listening ports that are used by QRadar, services, and components (continued)

Port	Description	Protocol	Direction	Required for
7789	HA Distributed Replicated Block Device (DRBD)	TCP/UDP	Bidirectional between the secondary host and primary host in an HA cluster	Distributed Replicated Block Device (DRBD) used to keep drives synchronized between the primary and secondary hosts in HA configurations
7800	Apache Tomcat	TCP	From the Event Collector to the QRadar Console	Real-time (streaming) for events
7801	Apache Tomcat	TCP	From the Event Collector to the QRadar Console	Real-time (streaming) for flows
7803	Apache Tomcat	TCP	From the Event Collector to the QRadar Console	Anomaly Detection Engine listening port
8000	Event Collection Service (ECS)	TCP	From the Event Collector to the QRadar Console	Listening port for specific Event Collect Service (ECS) events
8005	Apache Tomcat	TCP	None	This is a local port that is not used by QRadar.
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
10000	QRadar Web-based System Administration Interface	TCP/UDP	User desktop systems to all QRadar hosts	Server changes, such as the hosts root password and firewall access
23111	SOAP Webserver	TCP		SOAP Webserver listening port for the Event Collection Service (ECS)
23333	Emulex Fibre Channel	TCP	User desktop systems that connect to QRadar appliances with a Fibre Channel card	Emulex Fibre Channel HBAnywhere Remote Management service (elxmgmt)
32004	Normalized Event Forwarding	TCP	Bidirectional between QRadar components	Normalized event data communicated from an off-site source or between Event Collectors
32005	Data flow	TCP	Bidirectional between QRadar components	Data flow communication port between Event Collectors when located on separate managed hosts

Table 1-1 Listening ports that are used by QRadar, services, and components (continued)

Port	Description	Protocol	Direction	Required for
32006	Ariel queries	TCP	Bidirectional between QRadar components	Communication port between the Ariel Proxy server and the Ariel Query server
32009	Identity data	TCP	Bidirectional between QRadar components	Identity data communicated between the passive Vulnerability Information Service (VIS) and the Event Collection Service (ECS)
32010	Flow source listening port	TCP	Bidirectional between QRadar components	Flow listening port to collect data from QFlow Collector
32011	Ariel listening port	TCP	Bidirectional between QRadar components	Ariel listening port for database searches, progress information, and other associated commands
32000-33999	Data flow (flows, events, flow context)	TCP	Bidirectional between QRadar components	Data flows, such as events, flows, flow context, and event search queries
40799	PCAP data	TCP	From Juniper Networks SRX Series appliances to QRadar	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		Bidirectional traffic 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)

Viewing random port associations

Several ports allocate additional random port numbers for application services, for example, Message Queues (IMQ).

About this task

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.

Procedure

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

Login: **root**

Password: **<password>**

Step 2 Type the following command:

```
telnet localhost 7676
```

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

Searching for ports in use on QRadar

Netstat is a command-line tool used to determine which ports are in use on your QRadar Console or managed host.

About this task

The netstat command allows you to view all listening and established ports on the system.

Procedure

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

Login: **root**

Password: **<password>**

Step 2 Type the following command:

```
netstat -nap
```

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.

What to do next

For more information on netstat, type **netstat ?** for a list of available command-line parameters.

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.