

IBM QRadar Network Packet Capture
Version 7.3.0

Administration Guide



Note

Before you use this information and the product that it supports, read the information in [“Notices” on page 39](#).

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This document applies to IBM® QRadar® Security Intelligence Platform V7.3.0 and subsequent releases unless superseded by an updated version of this document.

© **Copyright International Business Machines Corporation 2016, 2018.**

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Introduction to QRadar Network Packet Capture product administration.....	v
Chapter 2. QRadar Network Packet Capture Administration.....	3
QRadar Network Packet Capture User accounts and authentication setup.....	3
Creating a new local user.....	3
Changing the local user password.....	4
Resetting the admin password by using the command line.....	4
Configuring Active Directory or an LDAP server for user authentication.....	5
Data consistency check during startup.....	6
Configuring date and time (NTP).....	6
Configuring location name and contact.....	9
Starting or stopping a packet capture.....	9
Configuring the remote syslog setup.....	10
Viewing syslogs.....	11
SNMP setup configuration.....	11
X509 configuration.....	11
Configuring the accelerator.....	11
Configuring prefilters	12
Setting up local retransmission.....	12
Clearing statistics or searches.....	13
Restarting the appliance and performing a factory reset.....	13
Configuring SSH.....	14
Chapter 3. QRadar Network Packet Capture and packet capture monitoring.....	15
Chapter 4. QRadar Network Packet Capture searches and queries.....	17
Queued searches.....	18
ACTIVE SEARCH	18
SEARCH HISTORY	18
Delete search.....	19
Berkeley packet filters.....	19
NTQL.....	23
Chapter 5. Grouped QRadar Network Packet Capture appliances.....	27
Group access.....	27
Group creation and modification.....	27
Setting up a QRadar Network Packet Capture group.....	28
Chapter 6. QRadar Network Packet Capture Stacking.....	31
Benefits of stacking appliances.....	31
Performance considerations.....	31
Creating a stack.....	32
Configuring a stack.....	33
Adding an appliance to an active stack.....	35
Removing an appliance from a stack.....	35
Maintaining existing stack nodes.....	36

Chapter 7. Troubleshooting with external LEDs.....	37
Notices.....	39
Trademarks.....	40
Terms and conditions for product documentation.....	40
IBM Online Privacy Statement.....	41
General Data Protection Regulation.....	41

Introduction to QRadar Network Packet Capture product administration

Administrators use IBM QRadar Network Packet Capture to manage the dashboard.

Intended audience

This guide is intended for all QRadar Network Packet Capture users responsible for investigating and managing network security. This guide assumes that you have QRadar Network Packet Capture access and a knowledge of your corporate network and networking technologies.

Technical documentation

To find IBM Security QRadar product documentation in the QRadar products library, see [Accessing IBM Security Documentation Technical Note \(www.ibm.com/support/docview.wss?rs=0&uid=swg21614644\)](http://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 \(http://www.ibm.com/support/docview.wss?uid=swg21616144\)](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 2. QRadar Network Packet Capture Administration

You can use the browser-based user interface to manage and configure your IBM QRadar Network Packet Capture appliance.

Default Admin user

The default admin user name is `admin` and the password is `pandion`.

Note: For security reasons, you should change the password for the admin user as soon as you are logged in. For more information about changing the password, see [“Changing the local user password” on page 4](#).

Secure connection

The QRadar Network Packet Capture appliance uses HTTPS to make the communication with the device secure. The appliance is factory-reset with a self-signed certificate. Your browser issues a warning that a self-signed certificate is in use that cannot be validated. Nevertheless, you can continue to the website.

To avoid a browser warning regarding the self-signed certificate, an administrator can install a custom certificate. For more information, see [“X509 configuration” on page 11](#).

QRadar Network Packet Capture User accounts and authentication setup

User authentication on the IBM QRadar Network Packet Capture appliance is a two-stage process. When a user tries to log in, authentication is done locally. If authentication fails, the user is authenticated against any configured Active Directory or Lightweight Directory Access Protocol (LDAP) server. If both types of authentication fail, the user is not granted access.

Note: If the QRadar Network Packet Capture appliance is member of a QRadar Network Packet Capture Group, the user account and authentication configurations are automatically synchronized across to the entire group.

Creating a new local user

If you have a small user base and don't need an authentication provider such as Active Directory or an LDAP server, create a local login account for each user that needs access to the IBM QRadar Network Packet Capture appliance.

Before you begin

Log in to the QRadar Network Packet Capture appliance as an administrator.

The QRadar Network Packet Capture unit also supports full user authentication as specified by configuring Microsoft® Active Directory or LDAP services, see [“Configuring Active Directory or an LDAP server for user authentication” on page 5](#).

Procedure

1. In QRadar Network Packet Capture, click the **ADMIN** tab
2. Go to the **ACCOUNTS** widget, and enter values in the **user** and **password** fields for the new user.
3. Select a user level:
 - For administrators who need the highest level of access and can change any configuration, select **Admin**.

- For users who need to use the QRadar Network Packet Capture appliance for operational uses, like searches and queries, select Operator.
- For users who only need to monitor results from the QRadar Network Packet Capture appliance, select Monitor.

Use the following information to determine the user level that you require:

Activity	Monitor level	Operator level	Admin level
Get statistics information from device	X	X	X
Get information about the current group setup	X	X	X
Start a search and query of data from the unit		X	X
Cancel an ongoing search		X	X
Change any configuration for the device including add or remove a user account			X
Reset/clear the statistics information of the unit			X
Get support information from the device including logs and support archive			X
Start and stop capturing of data			X
Change group setup			X

4. Click **Add account**.

Changing the local user password

For security reasons, you can change the password for any user by using the **ACCOUNTS** widget.

About this task

The local user is automatically logged out when you are changing the password. The user must log in again by using the new password. When an administrator changes their own password, they must also log in again.

Procedure

1. In QRadar Network Packet Capture, click the **ADMIN** tab.
2. Go to the **ACCOUNTS** widget, and type the relevant user name in the **user** field.
3. Type the new password in the **password** field and click **Update Account**.
A confirmation appears, and the new password takes immediate effect.

Resetting the admin password by using the command line

The recommended method for changing the local admin account password is by using the user interface (UI). However, since this method requires you to log in to the UI with the admin account, you might have to reset the admin account password by using the IMM2 command line interface (CLI).

Procedure

1. Establish a connection to the appliance by using a Telnet or SSH session.
2. Log in to the IMM browser and open a remote control session.
3. Log in to the Red Hat operating system as the `root` user.

The default password is `napatech10`.

4. Type this command to remove the accounts file:

```
rm /opt/pandion/service/pandion_rpcserver/conf/accounts.json
```

The admin user password is reset to the default password, which is pandion.

Configuring Active Directory or an LDAP server for user authentication

IBM QRadar Network Packet Capture integrates into your security infrastructure by using your existing authentication provider. Use the **AUTHENTICATION AND AUTHORIZATION** widget to configure Active Directory and LDAP. QRadar Network Packet Capture supports full user authentication as specified by Microsoft® Active Directory services or an LDAP server. Microsoft® Active Directory and LDAP servers as an authentication source are disabled by default.

Before you begin

Log into the QRadar Network Packet Capture unit as an administrator.

Procedure

1. Click the **ADMIN** tab, and go to the **AUTHENTICATION AND AUTHORIZATION** widget.
2. Select the appropriate **Server Type** and click **Apply**.

The parameters that you configure depend on the authentication server type.

Note: If the primary authentication and authorization server is inaccessible when a user requests authentication, a Service record (SRV) lookup is performed against the DNS name. The list of resolved SRV IP addresses is used as secondary authentication servers.

Important: If Active Directory is enabled, the user name must be a fully qualified domain name, for example, `\\[domain]\[user name]` or `[user name]@[domain]`.

Use the following table to choose and configure the correct **Server type**.

Parameter	Server Type	Description	Default
Protocol for communicating with the Active Directory or LDAP server	All	Protocol and encryption method. Possible values: <ul style="list-style-type: none">• LDAP• LDAP + TLS• LDAP + SSL	LDAP
Host name or IP address of the Active Directory or LDAP server	All		N/A
Port number to connect to on the Active Directory or LDAP server	All		389
Timeout in seconds of the connection to the Active Directory or LDAP server	All		25 seconds
Base Domain Name	All	The distinguished name where the query has to be started.	N/A
Administrator level group	All	Name of the group that is used to identify the admin level privileges	N/A
Operator level group	All	Name of the group that is used to identify the operator level privileges	N/A

Parameter	Server Type	Description	Default
Monitor level group	All	Name of the group that is used to identify the monitor level privileges	N/A
Filter	LDAP	The condition the entries must meet	N/A
Scope of the filter	LDAP	Possible values: <ul style="list-style-type: none"> • Base • One Level • Subtree 	Subtree
Attribute name used for assigning groups to users	LDAP	Name of the returned objects attribute that contains group names	
LDAP userbase used when binding to LDAP server	LDAP	Specify authentication information to allow users to log in with a short user name. For example, you can specify: cn={ },dc=company,dc=com where { } denotes the user name (for example, admin), and company.com is your domain. Another example might be: uid={ },ou=people, dc=company,dc=com When this USERBASE field is set, a user can log on using their short user name, (for example, admin) without needing to specify a fully qualified domain name.	

Data consistency check during startup

Stored data is checked for integrity and consistency during the startup of the IBM QRadar Network Packet Capture appliance.

A message is displayed after you log in to QRadar Network Packet Capture indicating that the service is initializing. A status bar at the top of the window shows the initialization progress.

The duration of the consistency check depends on the amount of data that are stored on the QRadar Network Packet Capture appliance.

Configuring date and time (NTP)

To ensure that captured data is time-stamped correctly, you must configure the date and time that QRadar Network Packet Capture uses. You can configure a local date and time for QRadar Network Packet

Capture, or you can enable Network Time Protocol (NTP) or Precision Time Protocol (PTP) to synchronize the date and time from an external source.

Before you begin

Ensure that a PTP cable is **not** connected to QRadar Network Packet Capture unit.

If you are modifying the time system from a previous setting, make sure you turn off the data capture before you install any updates.

If a significant time-jump (greater than one minute) is expected, restart the QRadar Network Packet Capture unit after the update to ensure that all the subsystems are synchronized.

If a negative time-jump is expected, erase all captured data before the update to avoid timestamp problems.

Procedure

1. Click the **ADMIN** tab, and go to the **NTP SETUP** widget.

TIME PROTOCOL SETUP

Current Date & Time
 2016-26-08 13:29:46 UTC
 2016-26-08 15:29:46 Local Time (GMT+0200)

Time service type

Server 1 address

Server 2 address

Server 3 address

Server 4 address

Status
 NTP not enabled

Configuration Section Controls

Figure 1: Time Protocol Setup widget

2. To configure a local time and date, enter date and time in the format that is described in the **Date & Time** field.
3. Choose a **Time service type** based on your requirements:

Table 1: Configuring time service type	
Time service type	Description
NTP	Synchronize the date and time with an external server.
RDate	Synchronize the current date and time from a network server.

Table 1: Configuring time service type (continued)	
Time service type	Description
Manual	Enter the date and time using either ISO8601 or dd/mm/yyyy h:m:s format.

4. Choose the relevant server addresses for the date and time sources.
5. Click **Apply** to complete.

Results

The accelerator in QRadar Network Packet Capture automatically synchronizes its time to the operating system time.

Configuring location name and contact

To make it easier to identify the QRadar Network Packet Capture appliance, ensure that you give it a recognizable name.

Procedure

1. Click the **ADMIN** tab.
2. Scroll down to the **GENERAL SETUP** widget, as shown below.

Figure 2: General Setup widget

3. Enter a Location name and optionally the name of a contact person.
4. Click **Apply**.

Starting or stopping a packet capture

You can control the number of recordings your appliance captures.

Procedure

1. In QRadar Network Packet Capture, click the **ADMIN** tab.
2. Go to the **CONTROL** widget.

3. Set **Traffic Capture** to **Turn On** or **Turn Off**.

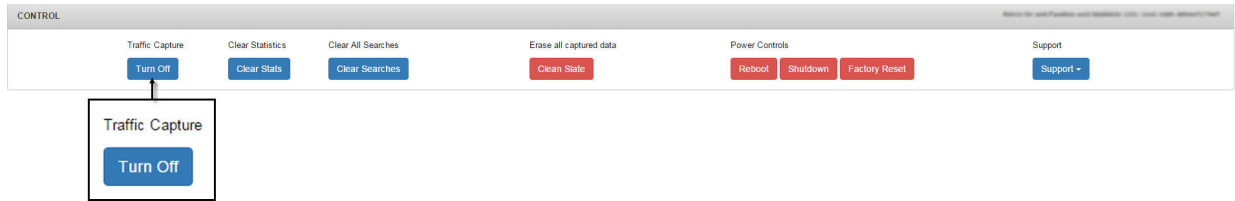


Figure 3: Traffic Capture

By default, the packet capture is turned on. If the QRadar Network Packet Capture is not capturing packets, then **Traffic Capture** is set to **Turn On**. If the QRadar Network Packet Capture is capturing packets, then **Traffic Capture** is set to **Turn Off**.

Configuring the remote syslog setup

Use the **REMOTE SYSLOG SETUP** widget to enable remote system logging and configure protocol details.

Procedure

1. In QRadar Network Packet Capture, click the **ADMIN** tab.
2. Go to the **REMOTE SYSLOG SETUP** widget.
3. Select the **Remote Syslog Enabled** check box to enable system logging.

The image shows the 'REMOTE SYSLOG SETUP' configuration page. It features a checkbox for 'Remote Syslog Enabled'. Below this, there is a 'Protocol' section with radio buttons for 'UDP' (selected) and 'TCP'. There are two text input fields: 'Remote Syslog Server Port' with the value '514' and 'Remote Syslog Server' with the value '0.0.0.0'. At the bottom, there are 'Apply' and 'Reset' buttons under the heading 'Configuration Section Controls'.

Figure 4: Remote Syslog Setup

4. Check the **UDP** or **TCP** protocol according to your settings.
5. Specify a port number for the **Remote Syslog Server Port** and an IP address for the **Remote Syslog Server** fields.

6. Click **Apply**.

Viewing syslogs

Use **SYSLOGS** to troubleshoot the device.

By default the **SYSLOGS** widget displays the last 500 lines of syslog in the IBM QRadar Network Packet Capture appliance.

You can filter and adjust the number of displayed lines by using the **Syslog Level** and **Log Lines** controls.

SNMP setup configuration

Use the **GUI SNMP SETUP** widget to set up SNMP for the QRadar Network Packet Capture appliance.

You can include the target IP address of where to send SNMP traps.

For more information about SNMP traps, see [Dell OpenManage SNMP Reference Guide Version 7.2](#) or search for *Dell OpenManage SNMP* in your preferred search engine.

X509 configuration

Use the **X509 SETUP** widget to install a new X509 certificate that is used by HTTPS to authenticate the IBM QRadar Network Packet Capture appliance.

A per device unique factory installed certificate is used when no user-installed certificate is present. The certificate is self-signed.

Configuring the accelerator

Use the **ACCELERATOR SETUP** widget to configure accelerator port settings, packet processing, and pre-filters.

Port Settings

If an SFP or SFP+ module is installed in a port, it is enabled by default. You can manually disable the module in the **ACCELERATOR SETUP** widget. By default, each port auto-detects the speed of the module. However, if you are using dual rate modules you can manually set the speed to 1G or 10G using the radio buttons.

The following table describes the function configuration for each port.

Port function setting	Description
Capture	Default setting. Packets are captured.
Disabled	Packet capturing is turned off, and no packets are captured.
Retransmit on ring	Packets are transmitted to another local port. Choose the port where you want the packets to be retransmitted.
Retransmit ETS	An ETS (Encapsulated Time Stamp) is appended to every packet, and all packets are retransmitted to another local port.

ACCELERATOR SETUP

Port	Function	Source	Link speed
Port 0	Capture		10G
Port 1	Capture		10G
Port 2	Capture		10G
Port 3	Capture		10G

PRE-FILTER

Advanced Pre-Filter

Submit advanced Pre-Filter to apply to capturing traffic.

Enable Slicing

Slicing Offset

No Dynamic Offset

Slice Offset

0

Configuration Section Controls

Apply

Reset

Figure 5: Accelerator Setup

Configuring prefilters

Use the **ACCELERATOR SETUP** widget to filter the packets that are captured to reduce the size of captured and stored packets.

Procedure

1. In QRadar Network Packet Capture click the **ADMIN** tab.
2. Go to the **ACCELERATOR SETUP** widget.
3. Configure prefilters:
 - a) Enter your statement in the **PRE-FILTER** field.
 - b) Click **Apply**.
4. Set up your packet processing:
 - a) Enter your statement in the **PRE-FILTER** field.
 - b) Select **Enable Slicing** and set the offset to enable slicing.
The slicing offset is configured as a dynamic offset plus a static offset so that all packets are sliced.
 - c) Click **Apply**.

Setting up local retransmission

By locally retransmitting traffic you can send any packet received on one network interface (a physical port) to one or more network interface. For example, you can retransmit all packets received on port 1 to port 2.

Insert the QRadar Network Packet Capture unit between an existing network tap and any network device. By enabling local retransmit you can receive all traffic into the QRadar Network Packet Capture unit and also forward all traffic to the connected network device.

Retransmission of a packet does not affect the capture of the packet.

The QRadar Network Packet Capture unit retransmits traffic to the selected ports.

Clearing statistics or searches

Use the **CONTROL** widget to clear all ongoing and queued searches.

Procedure

1. In QRadar Network Packet Capture, click the **ADMIN** tab.
2. Go to the **CONTROL** widget.
3. Set **Clear Statistics** to **Clear Stats** if you want to clear historical data.
4. Set **Clear All Searches** to **Clear Searches** if you want to clear all your recent searches.

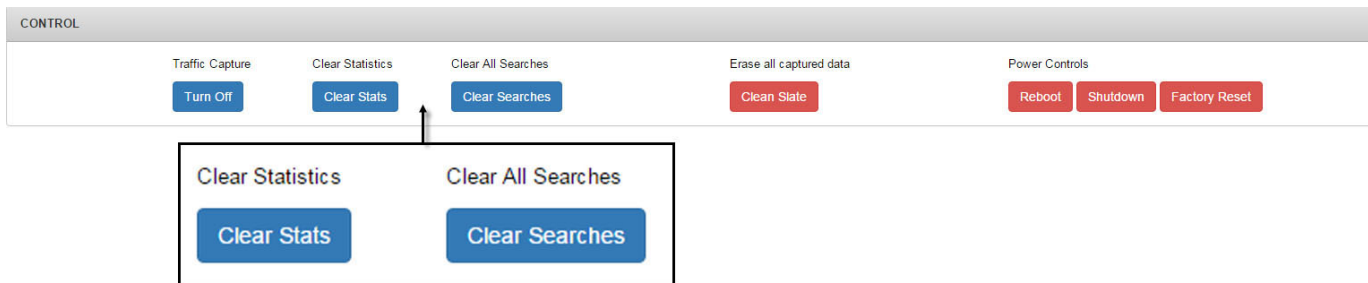


Figure 6: Clear Statistics or Searches.

Restarting the appliance and performing a factory reset

Use the **CONTROL** widget to access the IBM QRadar Network Packet Capture power settings.

Procedure

1. To restart or to shut down the QRadar Network Packet Capture appliance:
 - a) In QRadar Network Packet Capture, click the **ADMIN** tab.
 - b) Go to the **CONTROL** widget.
 - c) Set **Power Controls** to **Reboot** or **Shut Down**.

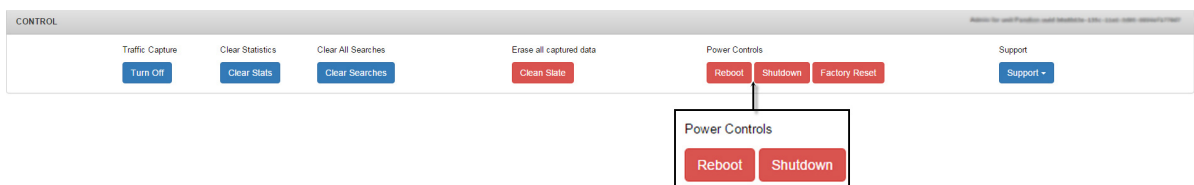


Figure 7: Power Controls

2. To erase network packets and perform a factory reset:
 - a) In QRadar Network Packet Capture, click the **ADMIN** tab.
 - b) Go to the **CONTROL** widget.
 - c) To erase network packets from the RAID disk array, under **Erase all captured data**, select **Clean Slate**.

Note: This action removes the data, but it is not a secure erase. It does not do multiple passes, not does it include secure wiping algorithms.

d) To reset the QRadar Network Packet Capture appliance, under **Power controls**, select **Factory Reset**.

Note: Factory Reset erases all captured data, and resets all settings with exception of the network configuration.

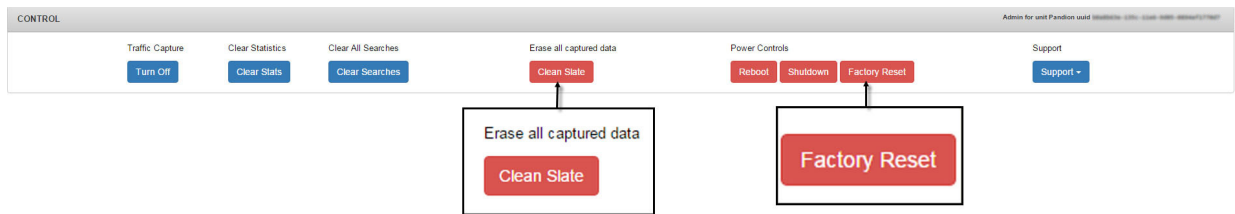


Figure 8: Power Controls

Configuring SSH

You can enable SSH command line access to help with troubleshooting and debugging. Use the **SUPPORT LOGIN (SSH)** widget to provide access to specific users. SSH support is always disabled by default. To allow SSH Support, a key certificate made available by customer support is required.

Procedure

1. In QRadar Network Packet Capture click the **ADMIN** tab.
2. Select **Support > Enable Support Login (SSH)** from the **CONTROL** widget

When SSH support is enabled, anyone with the key certificate and password can access the system for the active session (or until SSH is disabled by selecting **Support > Enable Support Login (SSH)**). When the host is rebooted, SSH is automatically disabled, and the user must re-enable SSH.

3. You can restrict SSH access to specific IP addresses by using the **SUPPORT LOGIN (SSH)** widget, by using the following steps:
 - a. Click the **ADMIN** tab.
 - b. Go to the **SUPPORT LOGIN (SSH)** widget.
 - c. Enter IP addresses one at a time, and click **Add**.

Results

SSH behavior changes as follows:

- Only addresses that have been specified are granted access to the system.
- SSH support is permanently enabled for these addresses; so SSH access is enabled by default after the appliance is restarted.

Chapter 3. QRadar Network Packet Capture and packet capture monitoring




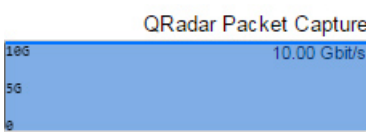
Use the Monitoring widgets on the **Dashboard** to view the overall status of one or more IBM QRadar Network Packet Capture appliances in a group.

A QRadar Network Packet Capture group consists of physically separate appliances, that capture data from separate network taps. Use grouping to form one logical entity that is easier to administer and search. A group can consist of up to eight QRadar Network Packet Capture appliances.

GROUP VIEW

Each QRadar Network Packet Capture appliance consists of the following monitoring components:

Table 3: Monitoring components

Icon	Description
	Accelerator
	System
	Storage
	Traffic

The state of the component is indicated by its color: light grey, yellow and red.

GROUP LIST VIEW

Use the **GROUP LIST VIEW** widget to monitor the health of each QRadar Network Packet Capture appliance in the group.

UNIT VIEW

Use the **UNIT VIEW** to see more detailed information about the IBM QRadar Network Packet Capture appliance selected in the **GROUP VIEW** widget.

The **UNIT VIEW** presents overview information about retention and appliance health for the QRadar Network Packet Capture appliance.

More detailed information displays about the **accelerator**, **system**, and **storage**.

CPU UTILIZATION

Use the **CPU UTILIZATION** widget to individually monitor the CPU usage for each hyper-threaded core. Identify the CPU by using the CPU model and speed that displays.

TRAFFIC

Use the **TRAFFIC** widget to monitor the history of the packet capture traffic that is received by the QRadar Network Packet Capture appliance.

The chart is updated periodically and scrolls to the right showing only the last period of historical data.

PACKET DISTRIBUTION

Use the **PACKET DISTRIBUTION** widget to monitor the distribution between broadcast, multicast and unicast frames that are received by the IBM QRadar Network Packet Capture appliance since the last reset of the statistics data.

PACKET SIZE DISTRIBUTION

Use the **PACKET SIZE DISTRIBUTION** widget to monitor the distribution of packet sizes for the frames that are received by the QRadar Network Packet Capture appliance since the last reset of the statistics data.

Chapter 4. QRadar Network Packet Capture searches and queries

To look for specific packets within a specific time range, and from a specific port, use the **SEARCH** tab. When you specify any combination of source IP, destination IP, source port, destination port or protocol fields a QRadar Network Packet Capture Query Language (NTQL) string is generated. You can modify the NTQL string, or you can create your own NTQL expression from scratch.

For example, to optimize NTQL, change `dst host` to `host`, or to change the `and` expression to an `or` expression between the source IP and destination IP addresses.

Limiting search results

To limit search results and reduce the time that it takes the search to deliver results, add scope to the search by using one of the following filters:

- Time Interval
- Receive Ports (selected ports)

If you are searching on a group of QRadar Network Packet Capture appliances, make sure that you submit search queries only when you logged on to the local appliance. Otherwise, retrieval performance of search results is impaired.

The format of the search output is in either standard PCAP format or PCAP-NG format. The PCAP-NG format contains port number information, even for searches across a group of QRadar Network Packet Capture appliances. For each server in the group, you can also specify the received ports to search for traffic.

FCS (Frame Check Sequence) information is also returned in this search output. This information is sent in addition to the packet data.

Before you submit the search, you can queue the search if the search engine is busy. You can choose whether or not the output should be automatically downloaded as soon as the search is completed, and you can prioritize different searches.

Differences between NTQL and BPF

Use NTQL to accelerate searches based on the index that is built during capture.

NTQL filters work differently than Berkeley Packet Filters (BPF). The following examples describe how NTQL filters work:

- When you search for an IP address, all packets that have this IP address are returned independent of any VLAN, MPLS or ISL tagging or encapsulation.
- When you search for specific TCP or UDP ports, the results that are returned include IPv6 packets with extended headers.

BPF post-filtering is based on the full BPF syntax. You create the BPF expression and this BPF post-filtering filters only the packets that passed the specified NTQL filter.

BPF filters work differently from the NTQL and might remove packets that was found by the NTQL filter.

Related concepts

[NTQL](#)

[Grouped QRadar Network Packet Capture appliances](#)

Queued searches

Queued searches are used when you have multiple searches that you want to run.

You can have only one ongoing search at a time, but you can run multiple searches, which are then queued and run according to priority. Queued searches are shown in the **SEARCH QUEUE** widget.

The following image shows a search query that is in a queued state, and will be run according to priority.

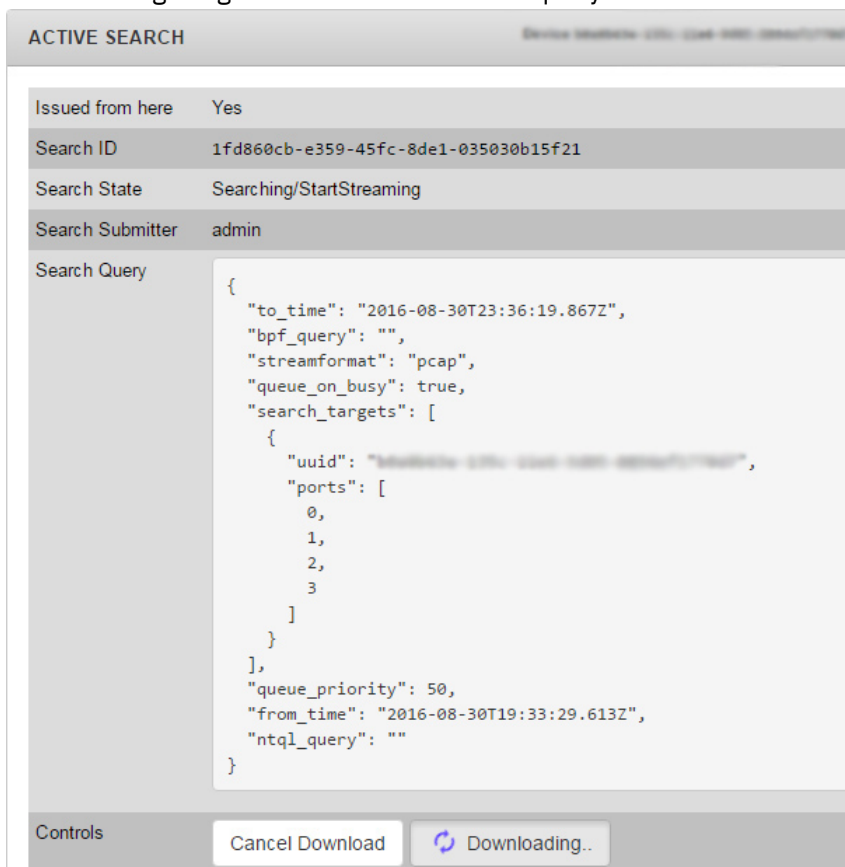
Figure 9: **SEARCH QUEUE** widget.

Before you submit the search, check the **Auto-download when ready to stream** option. The search result downloads automatically when the search is complete. You can change this behavior by clicking **Auto Download is On**.

ACTIVE SEARCH

Use the **ACTIVE SEARCH** widget to display any active and ongoing search.

The following image shows an active search query.



The screenshot shows the **ACTIVE SEARCH** widget interface. At the top, it displays the title "ACTIVE SEARCH" and a small URL. Below this, there is a table of search details:

Issued from here	Yes
Search ID	1fd860cb-e359-45fc-8de1-035030b15f21
Search State	Searching/StartStreaming
Search Submitter	admin

Below the table, the **Search Query** is displayed in a code editor. The query is a JSON object:

```
{
  "to_time": "2016-08-30T23:36:19.867Z",
  "bpf_query": "",
  "streamformat": "pcap",
  "queue_on_busy": true,
  "search_targets": [
    {
      "uuid": "1fd860cb-e359-45fc-8de1-035030b15f21",
      "ports": [
        0,
        1,
        2,
        3
      ]
    }
  ],
  "queue_priority": 50,
  "from_time": "2016-08-30T19:33:29.613Z",
  "ntql_query": ""
}
```

At the bottom of the widget, there is a **Controls** section with two buttons: "Cancel Download" and "Downloading..".

Figure 10: **ACTIVE SEARCH** widget.

SEARCH HISTORY

Use the **SEARCH HISTORY** widget to display the search history on the IBM QRadar Network Packet Capture appliance.

The following image shows the search history of a search query that has finished.

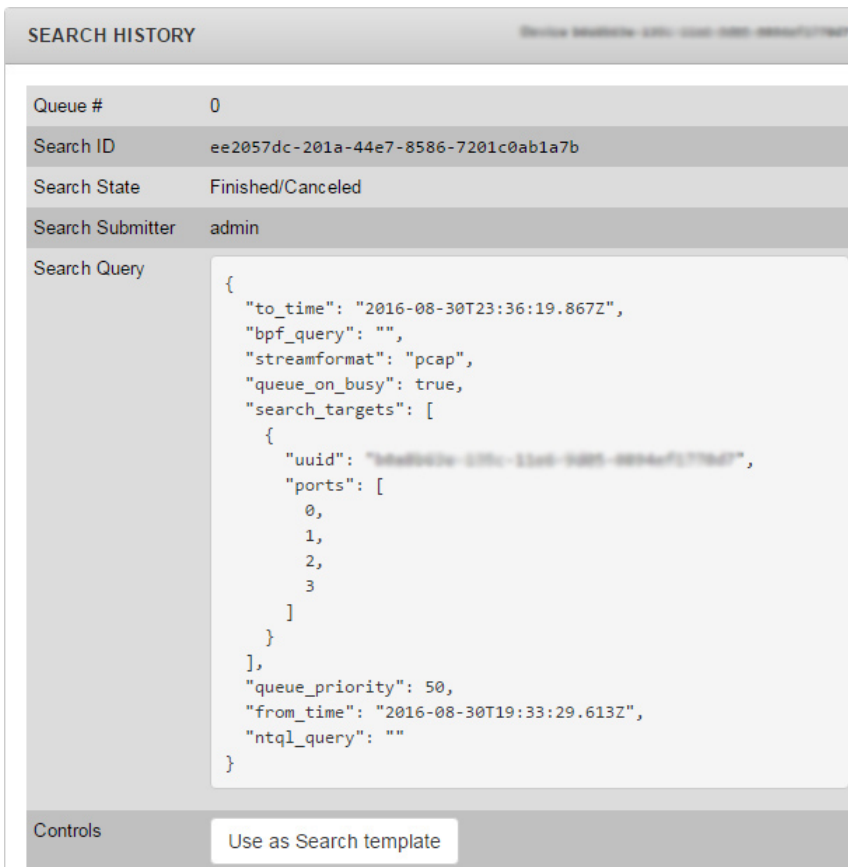


Figure 11: **SEARCH HISTORY** widget.

Search template

By using the **SEARCH HISTORY** widget, you can use a search that was previously run as a template for your next search. Click **Use as Search Template** and go to the **SEARCH** widget to make any necessary modifications to the template.

Delete search

You can stop a queued search by clicking **Cancel Queued Entry** in the **SEARCH QUEUE** widget. You can stop an active search by clicking **Cancel Search** in the **ACTIVE SEARCH** widget.

Berkeley packet filters

Berkeley Packet Filters (BPF) provide a powerful tool for intrusion detection analysis. Use BPF filtering to quickly reduce large packet captures to a reduced set of results by filtering based on a specific type of traffic. Both admin and non-admin users can create BPF filters.

Primitives

Primitives are references to fields in a network protocol header, such as host, port, or TCP port. The BPF syntax consists of one or more primitives, which usually consist of an ID, typically a name or number, which is preceded by one or more qualifiers.

Type qualifiers

Type qualifiers identify the kind of information that the ID name or number refers to. For example, the type might refer to host, net, port, or portrange. When no type qualifier exists, host is assumed.

Dir qualifiers

Dir qualifiers specify the transfer direction in relation to the ID. For example, the dir qualifier might be `src`, `dst`, or `src or dst`.

Proto qualifiers

The proto qualifier restricts the match to a particular protocol. Possible protocols are `ether`, `fddi`, `tr`, `wlan`, `ip`, `ip6`, `arp`, `rarp`, `decnet`, `TCP`, or `UDP`.

Primitive filter	Description
<code>[src dst] host <host></code>	<p>Matches a host as the IP source, destination, or either.</p> <p>The following list shows examples of host expressions:</p> <ul style="list-style-type: none">• <code>dst net 192.168.1.0</code>• <code>src net 192.168.1</code>• <code>dst net 172.16</code>• <code>src net 10</code>• <code>net 192.168.1.0</code>• <code>net 192.168.1.0/24</code>• <code>src net 192.168.1/24</code> <p>The host expressions can be used with other protocols like <code>ip</code>, <code>arp</code>, <code>rarp</code> or <code>ip6</code>.</p>
<code>ether [src dst] host <ehost></code>	<p>Matches a host as the Ethernet source, destination, or either.</p> <p>The following list shows examples of host expressions:</p> <ul style="list-style-type: none">• <code>ether host <MAC></code>• <code>ether src host <MAC></code>• <code>ether dst host <MAC></code>
<code>[src dst] net <network></code>	<p>Matches packets to or from the source and destination, or either.</p> <p>An IPv4 network number can be specified as:</p> <ul style="list-style-type: none">• Dotted quad (for example, <code>192.168.1.0</code>)• Dotted triple (for example, <code>192.168.1</code>)• Dotted pair (for example, <code>172.16</code>)• Single number (for example, <code>10</code>) <p>The following list shows some examples:</p> <ul style="list-style-type: none">• <code>dst net 192.168.1.0</code>• <code>src net 192.168.1</code>• <code>dst net 172.16</code>• <code>src net 10</code>• <code>net 192.168.1.0</code>• <code>net 192.168.1.0/24</code>• <code>src net 192.168.1/24</code>

Table 4: Primitive filters (continued)

Primitive filter	Description
[src dst] net <network> mask <netmask> or [src dst] net <network>/ <len>	Matches packets with specific netmask. You can also use /len to capture traffic from range of IP addresses. <ul style="list-style-type: none"> • Netmask for dotted quad (for example, 192.168.1.0) is 255.255.255.255 • Netmask for dotted triple (for example, 192.168.1) is 255.255.255.0 • Netmask for dotted pair (for example, 172.16) is 255.255.0.0 • Netmask for a single number (for example, 10) is 255.0.0.0 The following list shows some examples: <ul style="list-style-type: none"> • dst net 192.168.1.0 mask 255.255.255.255 or dst net 192.168.1.0/24 • src net 192.168.1 mask 255.255.255.0 or src net 192.168.1/24 • dst net 172.16 mask 255.255.0.0 src net 10 mask 255.0.0.0
[src dst] port <port> or [tcp udp] [src dst] port <port>	Matches packets that are sent to or from a port. Protocols, such as TCP, UDP, and IP, can be applied to a port to get specific results. The following list shows some examples: <ul style="list-style-type: none"> • src port 443 • dst port 20 • port 80
[src dst] portrange <p1>-<p2> or [tcp udp] [src dst] portrange <p1>-<p2>	Matches packets to or from a port in a specific range. Protocols can be applied to port range to filter specific packets within the range The following list shows some examples: <ul style="list-style-type: none"> • src portrange 80-88 • tcp portrange 1501-1549
less <length>	Matches packets less than or equal to length, for example, len <= length.
greater <length>	Matches packets greater than or equal to length, for example, len >= length.
(ether ip ip6) proto <protocol>	Matches an Ethernet, IPv4, or IPv6 protocol. The protocol can be a number or name, for example, <ul style="list-style-type: none"> • ether proto 0x888e • ip proto 50
(ip ip6) protochain <protocol>	Matches IPv4, or IPv6 packets with a protocol header in the protocol header chain, for example ip6 protochain 6.
(ether ip) broadcast	Matches Ethernet or IPv4 broadcasts

Table 4: Primitive filters (continued)

Primitive filter	Description
(ether ip ip6) multicast	Matches Ethernet, IPv4, or IPv6 multicasts. For example, ether[0] & 1 != 0.
vlan [<vlan>]	Matches 802.1Q frames with a VLAN ID of vlan. Here are some examples: <ul style="list-style-type: none"> • vlan 100 && vlan 200 filters on vlan 200 encapsulated within vlan 100. • vlan && vlan 300 && ip filters IPv4 protocols encapsulated in vlan 300 encapsulated within any higher-order vlan.
mpls [<label>]	Matches MPLS packets with a label. The MPLS expression can be used more than once to filter on MPLS hierarchies. This list shows some examples: <ul style="list-style-type: none"> • mpls 100000 && mpls 1024 filters packets with outer label 100000 and inner label 1024. • mpls && mpls 1024 && host 192.9.200.1 filters packets to and from 192.9.200.1 with an inner label of 1024 and any outer label.

Protocols and operators

You can build complex filter expressions by using modifiers and operators to combine protocols with primitive BPF filters.

Table 5: Protocols

Protocols		
<ul style="list-style-type: none"> • arp • ether • fddi • icmp • rarp 	<ul style="list-style-type: none"> • ip6 • ip • link • tcp • ppp 	<ul style="list-style-type: none"> • udp • wlan • slip • radio • tr

Table 6: Valid modifiers and operators

Description	Syntax
Parentheses	()
Negation	!=
Concatenation	'&&' or 'and'
Alteration	' ' or 'or'

BPF filter examples

The following table shows examples of BPF filters that use operators and modifiers:

BPF filter example	Description
<code>udp dst port not 53</code>	UDP not bound for port 53.
<code>host 10.0 .0.1 && host 10.0 .0.2</code>	Traffic between these hosts.
<code>tcp dst port 80 or 8080</code>	Packets to either of the specified TCP ports.
<code>ether[0:4] & 0xffffffff0f > 25</code>	Range based mask that is applied to bytes greater than 25.
<code>ip[1] != 0</code>	Captures packets for which the Types of Service (TOS) field in the IP header is not equal to 0.
<code>ether host 11:22:33:44:55:66</code>	Matches a specific host with that Mac address.
<code>ether[0] & 1 = 0 and ip[16] >= 224</code>	Captures IP broadcast or multicast broadcast that were not sent via Ethernet broadcast or multicast.
<code>icmp[icmptype] != icmp-echo</code>	Captures all icmp packets that are not echo requests.
<code>ip[0] & 0xf !=5</code>	Captures all IP packets with options.
<code>ip[6:2] & 0x1fff = 0</code>	Captures only unfragmented IPv4 datagrams, and frag zero of fragmented IPv4 datagrams.
<code>tcp[13] & 16 != 0</code>	Captures TCP-ACK packets.
<code>tcp[13] & 32 !=0</code>	Captures TCP-URG packets.
<code>tcp[13] & 8!=0</code>	Captures TCP-PSH packets.
<code>tcp[13] & 4!=0</code>	Captures TCP-RST packets.
<code>TCP[13] & 2!=0</code>	Captures TCP-SYN packets.
<code>tcp[13] & 1!=0</code>	Captures TCP-FIN packets.
<code>tcp[tcpflags] & (tcp-syn tcp-fin) != 0</code>	Captures start and end packets (the SYN and FIN packets) of each TCP conversation.

NTQL

Use QRadar Network Packet Capture Query Language (NTQL) to retrieve data from packets that are captured. For example, you can use NTQL for the following types of information:

- IPv4 host addresses, as source, destination or either
- IPv6 host addresses, as source, destination or either
- TCP or UDP port numbers, as source, destination or either
- Layer 3 protocol carried by Ethernet frames
- Layer 4 protocol carried by IP packages
- Combinations of these with logical AND and OR

Note: NTQL is case-sensitive.

Matching everything

An empty NTQL string matches all packets, which is useful when the number of matches is limited.

Host address search

To search for packets that were sent to a specific host, enter the following string:

```
src host <IP_address>
```

To search for packets sent from a host, enter the following string:

```
dst host <IP_address>
```

Port number search

To search for packets that were sent to or from a TCP or UDP port, enter the following string:

```
port <number>
```

Packets that are sent by using protocols that have no port numbers, are discarded by this search.

To narrow down the search results to packets that were sent from a specific port, enter the following string:

```
src port <number>
```

To search for packets that were sent to a specific port, enter the following string:

```
dst port <number>
```

Layer 3 protocol search

To search for packets that use a specific layer 3 protocol, enter the following string:

```
l3proto <protocol>
```

Where *<protocol>* is either a protocol number or a name. These are the supported protocol names:

- ip
- ip4
- ipv4
- arp
- ip6
- ipv6
- lldp
- ptp

When ip is specified as protocol, IPv4 is used.

Layer 4 protocol search

To search for packets that use a specific layer 4 protocol, enter the following string:

```
l4proto <protocol>
```

Where *<protocol>* is either a protocol number or a name. The following list describes the supported names are:

3pc, ah, argus, aris, ax.25, bbn-icc-mon, bna, br-sat-mon, cbt, cftp, chaos compaq-peer, cphb, cplx, crtp, crudp, dccp, dcn-meas, ddp, ddx, dgp, egp, eigrp

emcon, encap, esp, etherip, fc, fire, ggp, gmp, gre, hip, hmp, hopopt, i-nlsp, iatp icmp, idpr, idpr-cmtp, idrp, ifmp, igmp, igp, il, ip-in-ip, ipcomp, ipcu, ipip, iplt, ippc, iptm, ipv6, ipv6-frag, ipv6-icmp, ipv6-nonxt, ipv6-opts, ipv6-route, ipx-in-ip, irtp, iso-ip, iso-tp4, kryptolan, l2tp, larp, leaf-1, leaf-2, manet, merit-inp, mfe-nsp mhrp, micp, mobile, mobility header, mpls-in-ip, mtp, mux, narp, netblt, nsfnet-igp, nvp-ii ospf, pgm, pim, pipe, pnni, prm, ptp, pup, pvp, qnx, rdp, rohc, rsvp, rsvp-e2e-ignore, rvd, sat-expak, sat-mon, scc-sp, scps, sctp, sdrp, secure-vmtp, shim6, skip, sm, smp, snp, sprite-rpc sps, srp, sscopmce, st, stp, sun-nd, swipe, tcf, tcp, tlsp, trunk-1, trunk-2, ttp, udp, udplite uti, vines, visa, vmtp, vrrp, wb-expak, wb-mon, wesp, wsn, xnet, xns-idp,

Combining search terms

These search terms can be combined into more complex expression with AND and OR keywords. For example, to search for packets to OR from 192.0.2.1 or 192.0.2.2, enter the following string:

```
host 192.0.2.1 or host 192.0.2.2
```

To search for packets that are both to AND from 192.0.2.1 or 192.0.2.2, enter the following string:

```
host 192.0.2.1 and host 192.0.2.2
```

These keywords are left associative. For example, consider the following syntax:

```
port 42 and host 192.0.2.1 or host 192.0.2.2
```

The expression evaluates to the following:

- sent to or from port 42 and to or from host 192.0.2.1, or
- to or from host 192.0.2.2 without regard for the port numbers

You can change the left association by using parentheses, as shown in the following example:

```
port 42 and (host 192.0.2.1 or host 192.0.2.2)
```

The expression evaluates to find packets to or from port 42 that are to or from host 192.0.2.1 or 192.0.2.2.

Related concepts

[QRadar Network Packet Capture searches and queries](#)

Chapter 5. Grouped QRadar Network Packet Capture appliances

Use the IBM QRadar Network Packet Capture grouping feature to group multiple physical appliances together to form a single logical entity for administration and searching. By using the grouping feature, multiple tap points and multiple QRadar Network Packet Capture appliances can be accessed and operated as if they were one appliance.

A QRadar Network Packet Capture Group can capture data from separate network taps. You must configure all of the QRadar Network Packet Capture appliances to access all of the QRadar Network Packet Capture group members on the management network interface, and the network must have a DNS server.

When you group QRadar Network Packet Capture appliances, you can search all group members data with a single data query. The search result is a single PCAP file, that contains data merged from all group members.

You only need to log in to one of the members to access the entire group. From this single login, you can communicate by proxy with all other members of the QRadar Network Packet Capture group.

The proxy functionality is primarily intended for the administration, configuration and debugging of remote appliances. If a search is initiated that spans the whole group, while the user is on a remote QRadar Network Packet Capture through the proxy method, a significant amount of redundant traffic is transmitted across the management network. This impacts the retrieval performance depending upon the bandwidth and latency of the management network. Consequently, searches spanning a QRadar Network Packet Capture group must always be initiated on the primary or local machine, without any hub or proxying.

Related concepts

[QRadar Network Packet Capture searches and queries](#)

Group access

Some functionality works differently when you access an IBM QRadar Network Packet Capture appliance that is in a group.

Grouped appliances are different in the following ways:

- In the **GROUP VIEW** widget on the **DASHBOARD** tab, a number of QRadar Network Packet Capture appliances (the group) are visible.
- The **Switch To** button corresponds to the appliance switching in the GROUP VIEW on the DASHBOARD.
- When you modify user accounts and setup Active Directory, the updates are automatically propagated to all group members.

Group creation and modification

Initial peer-to-peer group

A grouping request is initiated on any IBM QRadar Network Packet Capture appliance, either through the GUI or the REST API.

In the following example, the QRadar Network Packet Capture appliance that requests the formation of a group is referred to as Appliance A. The receiver appliance of the grouping request is referred to as Appliance B.

For example, A QRadar Network Packet Capture group is formed with two members. The following things happen:

- As part of the grouping request, a user name and password with admin level access rights must be provided for Appliance B.
- The list of local accounts and Active Directory configuration is exported from Appliance A to Appliance B. All previous configurations of accounts and Active Directory configuration on Appliance B are overwritten.
- All capture data is preserved on Appliance A as well as on Appliance B, and can be searched from either appliance.

Inclusion in existing group

The request for a stand-alone QRadar Network Packet Capture appliance to be included in an existing group can be initiated on the stand-alone appliance or a member of the group. In the following example, the stand-alone QRadar Network Packet Capture appliance to be included in the group is referred to as Appliance C.

For example, when a QRadar Network Packet Capture appliance is included in an existing group, the following happens:

- Local accounts and the Active Directory configuration of the group are exported to Appliance C. Previous account and Active Directory configuration on Appliance C are overwritten.

Leaving a group

The local accounts and the Active Directory configuration are left as a snapshot of the state when a QRadar Network Packet Capture appliance is removed from a group. No further synchronization with the group occurs.

Setting up a QRadar Network Packet Capture group

Configure multiple QRadar Network Packet Capture appliance into a group.

Before you begin

- To be sure that you understand the implications of grouping a IBM QRadar Network Packet Capture appliances, see [Grouping of QRadar Network Packet Capture appliances](#).
- You are logged into the QRadar Network Packet Capture appliance as an administrator.

About this task

You can search the entire group, selected members, or a single member. The search result is delivered in a single merged stream that is in timestamp order. Each packet is annotated with the source device UUID and receive port in PCAP/NG format.

Procedure

1. Click the **ADMIN** tab, and navigate to the **GROUP MEMBERSHIP** widget.
2. Enter the DNS or IP address of the remote QRadar Network Packet Capture appliance.
3. Enter the login information of an admin user on the remote QRadar Network Packet Capture appliance.
4. Click **Add Host**.

Results

The remote QRadar Network Packet Capture appliance is grouped with the appliance that you are currently logged into.

What to do next

Click **Remove** to remove a QRadar Network Packet Capture appliance from the group.

Chapter 6. QRadar Network Packet Capture Stacking

You can extend the storage available for capture data by connecting multiple IBM QRadar Network Packet Capture appliances together in a ring topology to create a stack.

The stack allows the distribution of capture data across each of the connected appliances. It can connect up to 16 devices, but appears and behaves like a single entity that captures data from one TAP of a single 10GB port.

Stack controller

The Stack Controller is the appliance that receives the traffic that is being monitored, also known as the TAP point. The Stack Controller manages the overall configuration for the stack, therefore, there can be only one controller in each stack.

Stack node

The Stack Node is the appliance that is used as storage for the capture data. You can have up to 15 nodes in a stack.

Benefits of stacking appliances

Stacking gives you the ability to scale storage and expand retention time for capture data.

While the stack is actively capturing data, you can complete the following actions:

- Take an individual Stack Node offline, upgrade it, and reinsert it back into the stack.

Note: This capability does not apply to the Stack Controller.

- Add an appliance to expand the capacity of a stack.

The appliance hardware and storage size can vary. All available storage in the stack is used for data capture.

Data storage

The ring topology of the stack helps to protect the capture data. The capture data is stored in the stack by time frame; that is, an appliance holds all capture data for a certain time frame and overwrites the oldest data.

The time frame for the entire stack is established by concatenating all appliances in order. For example, in a stack with three appliances, Appliance A stores data from time frame 0-9, Appliance B stores data from time frame 10-19, and Appliance C stores data from time frame 20-29. As the appliances fill up with data, the oldest capture data is overwritten first. Appliance A now stores data from time frame 30 -39, overwriting data from time frame 0-9.

If an appliance goes offline, a gap in the capture data occurs, but the gap is limited to the time frame of the data that is held on the offline appliance. In the stack example, if Appliance B is offline, data from time frame 10-19 is not available, but all other capture data in the stack is available.

Performance considerations

The ring topology that is used to connect the stacked IBM QRadar Network Packet Capture appliances is designed to achieve high availability for continuous capture of data.

Each packet that is transmitted between the appliances includes extra data about the status of the stack. For example, the IP packets include information such as which stack node is storing data, the status of the stack nodes, and monitor the connectivity between the devices. Depending on your environment, the additional data that is transmitted with each packet might result in capture performance that is less the 10 Gbps under certain circumstances.

For example, network traffic that consists of a high proportion of small packets over time might result in a lower capture rate. While this situation is not typical for most deployments, if under these circumstances, your deployment requires full 10 Gbps capture, it is recommended that the QRadar Network Packet Capture appliances be deployed stand-alone instead of using a stack.

Creating a stack

Create a new physical QRadar Network Packet Capture stack to increase the storage space that is available for your capture data.

Before you begin

Prepare your environment before you create the stack.

- You can stack a maximum of 16 appliances, including the Stack Controller. The maximum physical cabling distance between any two appliances is ten meters.
- Ensure that all appliances in the stack are running the same version of the QRadar Network Packet Capture software.
- Ensure that all appliances are in a group. For more information, see [Grouped appliances](#).
- Interconnect the appliances to form a ring so that all appliances can communicate with each other. To see an example cabling diagram, see [Stacking topology](#).

Note: Routing and switching are not allowed. Only peer-to-peer connections are allowed.

Procedure

1. On the Stack Controller, connect Port 2 to the switch or SPAN port that is being monitored; this is the TAP point.
2. On the Stack Controller, connect Port 3 to a QRadar QNI appliance.
Port 3 is used to retransmit all capture data to the QNI appliance. The data is retransmitted in a special format with a high-precision data capture time stamp that is embedded in the frame.
3. On the Stack Nodes, connect port 0 and port 1 to form a ring.

Note: For the Stack Nodes, Ports 2 and 3 must not be used.

Example

The following diagram shows a sample topology with a Stack Controller (Appliance A) and three Stack Nodes (Appliances B, C, and P).

The NT40E3-4 ports are connected by using ports 0 and 1 to form a ring.

1. Appliance A, Port 0 connects to Appliance B, Port 1.
2. Appliance B, Port 0 connects to Appliance C, Port 1.
3. Appliance C, Port 0 connects to Appliance A, Port 1.

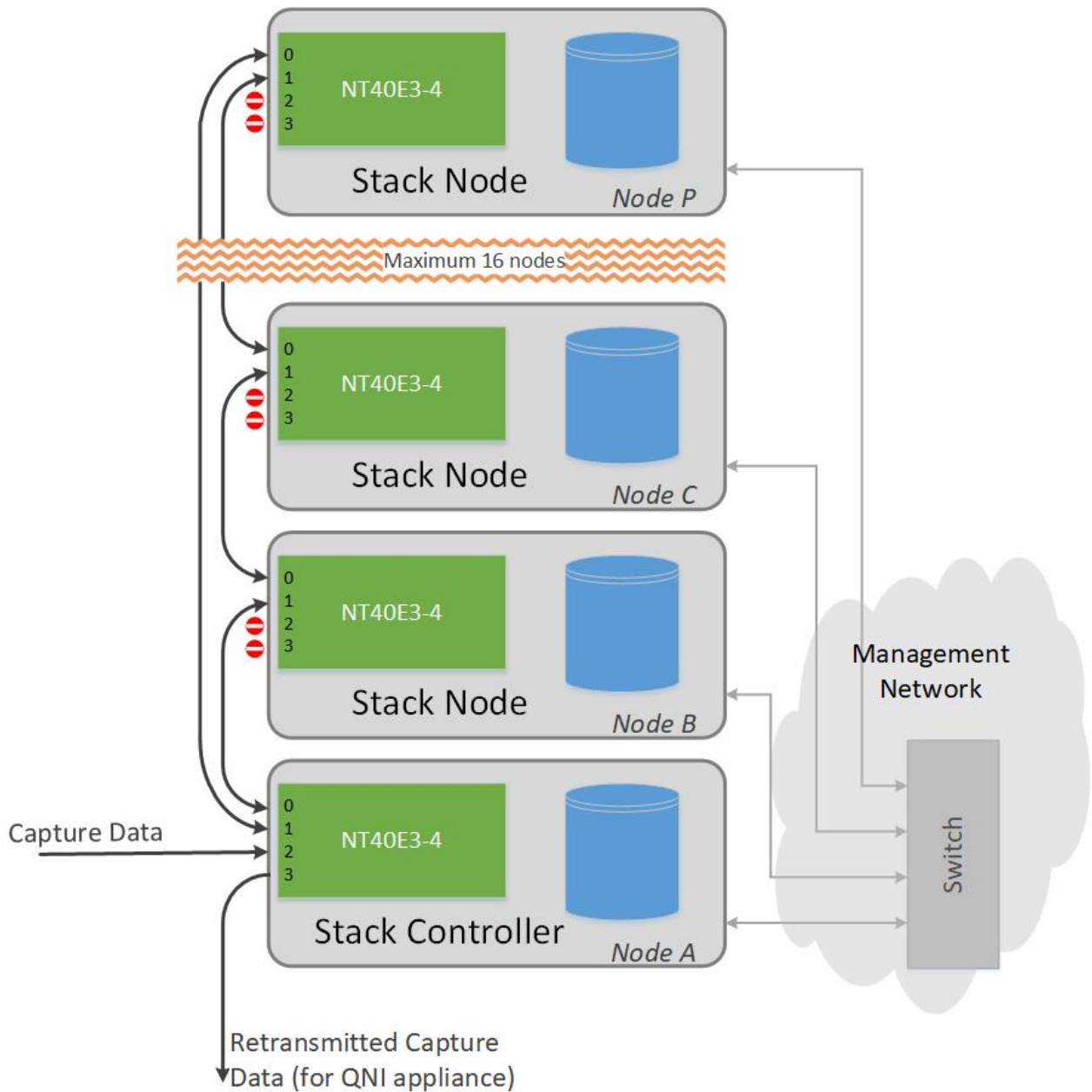


Figure 12: QRadar Network Packet Capture sample topology.

Configuring a stack

Use the **STACKING** widget to configure the stack.

Before you begin

If an appliance contains capture data that is not relevant to the stack that you are adding it to, remove the captured data from the appliance before adding it to the stack.

About this task

The **STACKING** widget displays the configuration of the stack. The following image shows a stack that is fully configured and capturing data:



Figure 13: Configuring a stack.

Only one appliance at a time is capturing data. As the appliance fills up with capture data, a different appliance in the stack becomes the **Storing** appliance.

The order in which appliances are enabled for capture is random. Neither the order of devices in the **STACKING** widget view or the physical cabling influences the selection order. However, when all appliances in the stack hold capture data, the next capturing device is always the appliance that holds capture data with the oldest time stamp.

Procedure

1. Click the **ADMIN** tab and open the **GROUP MEMBERSHIP** widget.
Verify that all appliances for the stack are correctly grouped.
2. Assign a Stack Controller and create the stack:

- a) In the **STACKING** widget, in the **Stack Controller** list, select the appliance that you want to be the Stack Controller.

The stack name is used only to uniquely identify the stack, and is not used anywhere else in the configuration.

- b) In the **Name of new stack** field, type a descriptive name for the Stack Controller, and then click **New Stack**.

The new stack is created and appears as a new entry in the **STACKING** widget.

3. Add stack nodes to the stack:

- a) In the **Unit to add** list box, select the appliance that you want to add to the stack.
- b) In the **Stack** list, select the name of the stack that you want to add the appliance to, and click **Add Stack Node**.

If a group contains multiple stacks, ensure that you select the correct stack name from the menu.

- c) Repeat these steps for each appliance that you want to add to the stack.

When all appliances are added, the stack should appear healthy and ready to enable data capture.

Note: When you add Stack Nodes, the operational status of the **STACKING** widget might show temporary Operational Status errors. This happens because connectivity in the stack ring is incomplete until all Stack Nodes are added.

4. Verify the stack configuration:

- a) Select the stack and verify that the list of appliances is as expected for the stack.
- b) Check that each appliance in the stack has the same version number and displays the following values:
 - **Operational Status** = OK
 - **State** = In Service

You are now ready to enable data capture.

5. Turn on data capture:

- a) Click **Expect** next to each Stack Node in the stack to enable the appliance for data capture.

Note: By default, all Stack Nodes are set to **Unexpect** when they are first added to the stack to prevent an appliance storing captured data until it is physically enabled.

- b) Go to the **GROUP MEMBERSHIP** widget, and click **Switch To** for the relevant Stack Controller.
- c) Go to **Traffic Capture**, and click **Traffic Capture** to start capturing data.
- d) Click the **DASHBOARD** tab for the Stack Controller to check for ingress traffic.

Port 2 of the Stack Controller is the TAP port for the stack. If there is ingress traffic on this port, you see:

- 1) The traffic pattern matches the ingress traffic.
- 2) The traffic pattern on the Stack Controller dashboard for all Stack Nodes is twice the size of the ingress traffic (plus a number of 64-127 bytes unicast packets).

Note: The ingress traffic is transmitted to all appliances in the stack, but in both directions (clockwise and counterclockwise) on port 0 and port 1. At the same time, a proprietary stack protocol is running that continuously carries several small frames across the ring.

6. Check the capture data in the **STACKING** widget:

- a) Check the appliances in your stack and find the appliance whose **Capturing** column shows a value of **Storing**.

Only one appliance at a time is capturing data, therefore, only one appliance shows **Storing** and all other appliances are idle.

- b) On the appliance that is capturing data, check that the **First packet** and **Last packet** columns show valid time stamp values.

As the appliance fills up with capture data, a different appliance in the stack becomes the Storing appliance, and the **First packet** and **Last packet** time stamps for the new appliance are updated.

Adding an appliance to an active stack

You can expand the capacity of a stack by adding appliances while the stack is actively capturing data.

Procedure

1. Install a QRadar Network Packet Capture appliance with the same version of software as the appliances in the stack that you want to expand.
2. Complete the physical installation of the appliance.

This process includes attaching the appliance to the common management network, breaking up the stack ring, and cabling the new appliance into the ring. You can put the new appliance in any physical location in the stack. For more information, see [“Creating a stack” on page 32](#).

Note: During this process, connectivity in the stack ring is incomplete, and the operational status of the **STACKING** widget might show temporary cabling errors.

3. Include the new appliance in the group, and add it to the stack as described in [Add a Stack Node \(Step 3\)](#).
4. Check the **STACKING** widget to view the status of the new appliance.

The appliance is fully operational when the **Operational Status** shows **OK**, the **First packet** and **Last packet** settings show **N/A**, and no cabling errors remain.

When the appliance that is capturing data is full, the stack switches to the newly inserted appliance for data capture.

Removing an appliance from a stack

When you remove an appliance from the stack, the capture data on the appliance is retained. You can run local searches on the appliance to access the data.

Procedure

To permanently remove an appliance from a stack, select the appliance and click **Remove** in the **STACKING** widget.

Note: You cannot remove the Stack Controller until all Stack Nodes are removed from a stack.

What to do next

Physically remove the cabling from the appliance, and re-cable the stack ring. You may see temporary cabling errors while stack connectivity is re-established.

Maintaining existing stack nodes

You can put a Stack Node in standby mode to allow for upgrades and maintenance while the remaining stack is active. With this capability, you can upgrade each of your Stack Nodes, while the in-service appliances continue to capture data.

Before you can upgrade the Stack Controller, you must disable data capture and take the entire stack offline.

Before you begin

Ensure that you update all Stack Nodes before you update the Stack Controller.

About this task

When an appliance is in standby mode, you can upgrade the operating system and application software of the appliance. If the appliance does not need to be restarted, connectivity between the appliance and the stack ring is maintained. If the appliance is actively capturing data when standby mode is enabled, the stack switches immediately to another appliance for active capture.

If an update affects communications with the Stack Controller, for example an update to protocols, the Stack Nodes can handle this during the update process because they are backward compatible with protocols and commands that are sent from the Stack Controller.

A Stack Node in standby mode has the following characteristics:

- Continues to appear in the stack list in the **STACKING** widget.
- Maintains stack ring connectivity.
- Maintains group membership.
- Includes capture data in searches.
- Is not used as an active capture device in the stack; new data is not captured to this appliance.

You cannot put the Stack Controller into standby mode without a service interruption because it is the only appliance that has the TAP port, and it distributes the data to all appliances in the stack.

Procedure

1. In the **STACKING** widget, select the appliance that you want to work with, and then click **Standby**.

Note: To allow the maximum time to apply updates to the appliance, select the stack node that has the newest **First packet** and **Last packet** time stamp, but that is not currently capturing data.

2. Apply the updates to the standby appliance.
3. When the maintenance is complete, in the **STACKING** widget, select the appliance and then click **In Service** to re-enable it.

Chapter 7. Troubleshooting with external LEDs

Use the state and color of the external LEDs to help you troubleshoot your IBM QRadar Network Packet Capture appliance.

Use the information in the following image and tables to help you locate the various external LEDs and troubleshoot problems.

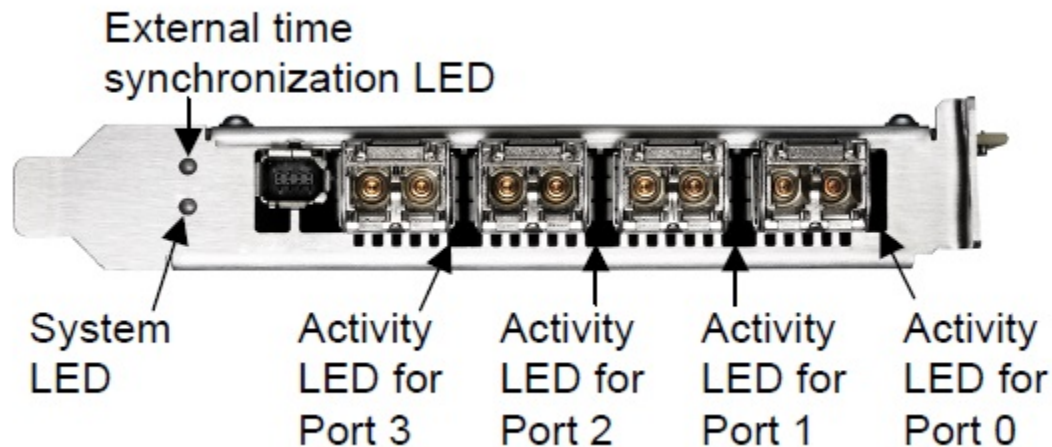


Figure 14: Location of the external LEDs

Activity LEDs

The following table describes the typical states that are indicated by the color of the Activity LEDs.

State and Color	Condition
Off	The driver is not loaded, the Ethernet link is down, or the port is disconnected.
Constant green	The driver is loaded and the Ethernet link is up, but there is no traffic.
Flashing green	The driver is loaded but there is traffic on the Ethernet link.

System LED

The following table describes the typical states that are indicated by the color of the System LED.

State and Color	Condition
Off	The power is off.

Table 9: System LED and operating status of the appliance. (continued)

State and Color	Condition
Constant red	During start-up and the power is on, the accelerator is checking the power supplies.
Flashing red	After start-up and the power is on, there is an unrecoverable hardware error.
Constant yellow	During start-up the power is on, and the power supplies are working.
Flashing yellow	There is a new entry in the hardware log.
Constant green	The FPGA is loaded, and the system is running.

External time synchronization LED

The following table describes the typical states that are indicated by the color of the external time synchronization LED.

Table 10: External time synchronization LED and the operating status of the appliance.

State and Color	Condition
Off	No driver is loaded or the Ethernet link on the Precision Time Protocol (PTP) port is down.
Constant yellow	The Ethernet link on the PTP port is up.

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>.

General Data Protection Regulation

Clients are responsible for ensuring their own compliance with various laws and regulations, including the European Union General Data Protection Regulation. Clients are solely responsible for obtaining advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulations that may affect the clients' business and any actions the clients may need to take to comply with such laws and regulations. The products, services, and other capabilities described herein are not suitable for all client situations and may have restricted availability. IBM does not provide legal, accounting or auditing advice or represent or warrant that its services or products will ensure that clients are in compliance with any law or regulation.

Learn more about the IBM GDPR readiness journey and our GDPR capabilities and Offerings here: <https://ibm.com/gdpr>

