IBM QRadar
7.4.3

Hardware Guide

Note

Before you use this information and the product that it supports, read the information in “Notices” on page 89.

Contents

About this guide

The IBM® QRadar® SIEM Hardware Guide provides QRadar appliance descriptions, diagrams, and specifications.

Intended audience

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

Technical documentation

For information about how to access more technical documentation, technical notes, and release notes, see Accessing IBM Security Documentation Technical Note (http://www.ibm.com/support/docview.wss?rs=0&uid=swg21612861).

Contacting customer support

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

Statement of good security practices

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

Please Note:

Use of this Program may implicate various laws or regulations, including those related to privacy, data protection, employment, and electronic communications and storage. IBM 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 QRadar.

Chapter 1. QRadar SIEM hardware migration scenarios

If your hardware reaches its end of life, you need to be able to process more events of flows, or you are consolidating existing hardware, plan to migrate data from older IBM QRadar SIEM appliances to new QRadar appliances.

You have several options when you migrate:

Replacing a QRadar managed host

Migrate data from an older IBM QRadar managed host (16xx, 17xx, or 18xx) appliance to newer hardware.

Before you begin

Ensure that the following conditions are met:

- You recorded the network information for the old appliance. You must manually type this information into the network configuration for the new appliance.
- The software version of the new appliance matches the software version of the QRadar Console. You might have to reinstall an ISO image for the appliance to downgrade or use an SFS fix pack to upgrade.
- You configured data backups to prevent potential data loss during the migration.

About this task

Follow this process for non-HA appliances. If you need to replace an appliance in a high-availability (HA) cluster, you must first remove the HA appliance from the cluster.

During migration, the IP address of the old appliance is assigned to the new hardware. The new hardware is added to the deployment and then you move data while new events are collected from the network.

Procedure

1. Prepare your new hardware:
   a) Rack the appliance and connect network connections.
   b) Review the paperwork for your appliance to determine which QRadar version is installed on the new hardware.
2. Review your software version.
   a) If your Console software version is older than the software on the appliance, reinstall the appliance with the newest ISO that is less than or equal to the Console software version. Download the ISO file from Fix Central (www.ibm.com/support/fixcentral/).
   b) Follow the installation wizard to complete the installation.
   c) Type a root password for the appliance.
   d) Type a temporary IP address and network information for the new hardware.
   e) Log in as a root user, and select the appliance type during the installation process.
   f) If your Console patch version is newer than the software on the appliance, download and install the SFS (software fix/patch) from Fix Central (www.ibm.com/support/fixcentral/).
3. Remove the old appliance from the deployment.

a) Log in to QRadar as an administrator.

b) Click the **Admin** tab and click the **System and License Management** icon.

c) From the Display menu, click **Systems**, and then select the old QRadar appliance.

d) Click **Deployment Actions** > **Remove Host**.

e) When prompted, click **Remove** to confirm the removal of the host deployment.

Attention: Don't delete the components for the Event Collector, and Event Processor, because these components are reused.

Note: Verify all external storage that is not `/store/ariel` or `/store` is not mounted.

4. Reassign the IP addresses to ensure that the decommissioned appliance doesn't cause an IP address conflict in the network after it is powered back on.

a) To reassign the IP address of the old appliance to any unused address:

i) Use IMM (Integrated Management Module) for remote access, or use the local Console keyboard, to log in to the command line of the old appliance as the root user.

ii) Reassign the IP address of the old appliance by typing the following command:

```
/opt/qradar/bin/qchange_netsetup
```

b) Set the IP address for the new hardware:

i) Use IMM for remote access, or use the local Console keyboard to log in to the command line of the new appliance as the root user.

ii) From the command line of the new appliance, type `/opt/qradar/bin/qchange_netsetup` to use same host name and IP address as the old appliance.

If you want to migrate old data to the new system, leave the existing system running and connected to the network. The data is moved when the new appliance is running and collecting data.

5. Add the new appliance to the deployment

a) Log in to QRadar as an administrator.

b) Click the **Admin** tab and click the **System and License Management** icon.

c) Click **Deployment Actions** > **Add Host**.

d) If you're prompted to add old components from the deployment to the host, click **Yes**. Any deployment components that were on the old appliance are reassociated with this host so that any protocol-based sources are automatically enabled and migrated to the new appliance.

e) Click **Save and Close**.

f) On the **Admin** tab, click the **Deploy Changes** icon.

g) Verify that event or flow sources that were reporting to the original host are being processed in the QRadar user interface.

After you add the host back to the QRadar deployment, the deployment process ensures that the required configuration is regenerated on the new appliance. After the new host is part of the deployment, you can only use SSH access from the Console.

6. To copy data from the old appliance, you shut down the host firewall on the new appliance by typing the command `systemctl stop iptables`.

7. To migrate data nodes, follow these steps.

a) On the data nodes that are not being replaced, ensure that you have enough disk space to store the imported data until the migration is complete.

b) Select the Data Node appliance in the host table, and on the **Deployment Actions** menu, click **Edit Host**.

c) Click the **Component Management** settings icon (⚙). In the **Data Node Mode** field, select **Archive**, and then click **Save**.

d) On the **Admin** tab, click **Deploy Changes**.

e) On the **Deployment Actions** menu, click **Add Host**.

f) Configure the settings for the managed host, and then click **Add**.

g) Select the new Data Node appliance in the host table. On the **Deployment Actions** menu, click **Edit host**.

h) Click the **Component Management** settings icon (⚙). In the **Data Node Mode** field, select **Archive**, and then click **Save**.

i) On the **Admin** tab, click **Deploy Changes**.

j) For each old data node, migrate the data to a new data node.

k) Set the new data nodes to **Active** mode.

l) Select the old Data Node appliance in the host table. On the **Deployment Actions** menu, click **Remove host**, and then click **OK**.

m) On the **Admin** tab, click **Advanced** > **Deploy Full Configuration**.

8. Copy certificates and custom-generated key pairs from the old appliance to the new appliance to ensure that log sources and scanners can connect to remote sources.

   You must also migrate any custom generated private keys that you have by transferring the `/etc/ssh` and `/root/.ssh` directories.

   a) Log in to the old QRadar managed host as the root user.

   b) Copy the data from the old hardware to the new appliance by using the **`rsync`** command as in one of the following examples:

   Tip: For better performance when using a crossover cable solution, use rsync -av instead of rsync -avz.

   Use this example for certificates:

```
Example: rsync -avz /opt/qradar/conf/trusted_certificates/
   root@new_appliance:/opt/qradar/conf/trusted_certificates
```

   Use these examples for SSH:

```
Example 1: rsync -avz /etc/ssh/ root@new_appliance:/etc/ssh
```

```
Example 2: rsync -avz /root/.ssh/ root@new_appliance:/root/.ssh
```

9. Transfer event and flow data to the new appliance.

   You can use either **`rsync`** or **SCP** to complete the data transfer. These commands might require the root user to accept SSH keys and provide the root password for the target server. The length of this process depends on how much data needs to be transferred.

   a) Log in to the old QRadar appliance as the root user.

   b) Copy the data from the old appliance to the new appliance (target server) by using the **`rsync`** command, as in the following example:

   Tip: For better performance when you use a crossover cable solution, use **`rsync -av`** instead of **`rsync -avz`**.

```
rsync -avz /store/ariel/ root@new_appliance:/store/ariel
```

10. Optional: Copy over event collector data, if you have any data in `/store/ec`.

    a) Log in to the old appliance as the root user.

    b) Stop ecs-ec-ingress on the old appliance by typing the following command:

```
systemctl stop ecs-ec-ingress
```

c) Log in to the new appliance as the root user.

d) Create a file on the new appliance to prevent ecs-ec-ingress from automatically restarting by typing the following command:

```
touch /storetmp/ecs-ec-ingress.ecs-ec-ingress.manually_stopped
```

e) Stop ecs-ec-ingress on the new appliance by typing the following command:

```
systemctl stop ecs-ec-ingress
```

f) Copy the data from `/store/ec` on the old appliance to `/store/ec` on the new appliance.

g) Remove the file that is created in substep d from the new appliance by typing the following command:

```
rm -f /storetmp/ecs-ec-ingress.ecs-ec-ingress.manually_stopped
```

h) Start ecs-ec-ingress on the new appliance by typing the following command:

```
systemctl start ecs-ec-ingress
```

11. Type the command `systemctl start iptables` after the configuration and data migration are complete.

What to do next

After the data transfer is complete, decommission the old appliance and unrack the obsolete hardware.

Replacing a QRadar Console with an appliance that uses the same IP address

Migrate data from an older IBM QRadar Console to a new console that uses the same IP address. All managed host appliances stay as-is. Use this process for non-HA appliances.

Before you begin

- Write down the network information for the old Console; you must enter this information into the network configuration for the new appliance. Ensure that the old Console and the new Console are in the same network.
- Save a recent configuration backup from the old Console. The configuration backup is used to restore settings, users, rules, log sources, and more to the new Console.
- Complete a QRadar installation on the new Console by using the software version that matches that of the old Console. The installation of the new Console uses a temporary IP address until the old hardware is removed from the deployment.
- If you are using WinCollect, ensure that the WinCollect version on the new Console matches the version on the old Console before you migrate.

About this task

It is not necessary to remove managed hosts from the old QRadar Console because the new QRadar Console takes over any existing hosts in the deployment. This procedure allows managed hosts in the deployment to continue to receive events while the Console is offline.

Important: App data is separated from the configuration backup and restore. To backup and restore app data, see Backing up and restoring app data.

Procedure

1. Prepare your new hardware:
   a) Rack the appliance and connect network connections.
   b) Turn on the appliance and log in as a root user.
   c) When the system displays the license agreement (EULA), press **Ctrl+C** to open a command prompt.
   d) To view the installed software version, type the following command:

   ```
   /opt/qradar/bin/myver
   ```

   e) Compare the software version on the new hardware and the old hardware:
      - If the new hardware's software version is older than the software that is running in production, log out, and then log in again as the root user and complete the installation. After the installation completes, download the correct Fix Pack to upgrade the Console to the same version as the deployment.
      - If the new hardware's software version is newer than the software that is running in production, you can either choose to upgrade your production system to match the new appliance, or downgrade the software by installing an older release of QRadar from Fix Central (www.ibm.com/support/fixcentral/). Reinstall the new system with an older release first, and then begin this procedure.
      - If the new hardware's software version is the same as the software that is running in production, log out, log in again as root, and complete the installation.
   f) Configure QRadar.
   g) Type a temporary IP address and network information for the new hardware.
   h) Type a root password for the appliance.
   i) Follow the installation wizard to complete the installation.
   j) If required from Step 1e, upgrade the new hardware to the same version level as the old Console.
2. Prepare your old QRadar hardware:
   a) Log in to the old Console.
   b) Click the **Admin** tab, and then click the **Backup and Recovery** icon.
   c) From the navigation menu, click **On Demand Backup**.

      Important: Configuration backups can only be restored to the same version of QRadar that they were created with. If you plan to change the overall QRadar version in the deployment, you must create a new configuration backup after any software change and keep these files in a safe place for your hardware migration. Moving from a smaller Console to a larger or newer appliance is supported by the migration or backup process. For example, a 3105 Console's configuration backup can be applied to a 3128 or a 3148 appliance.
   d) Type a name and description for the new configuration backup.
   e) Click **Run Backup** and wait for the configuration backup to complete.
   f) After the backup finishes, click the new configuration backup name that you created to download the file.
   g) Copy the configuration backup from the old QRadar Console to a safe location.
   h) Stop services on the old Console by typing the following commands:

   ```
   systemctl stop hostcontext
   systemctl stop tomcat
   systemctl stop hostservices
   systemctl stop tunnel_manager
   ```

   A configuration backup file is created for the new Console to use. This file is required later on in the procedure to restore users, rules, log sources, offenses, reports, admin configurations, and other system settings to the new hardware.

3. Reassign IP addresses on the old QRadar Console.

   This process is done manually by adjusting the network configuration file directly, instead of using the `qchange_netsetup` command. You can use this method to change the system's physical IP address to avoid conflicts. If the backup restore does not complete on the new system, you can easily revert to the old address. After the IP address is changed on the existing console, it cannot affect any changes to the other hosts in the deployment unless the IP address is reverted.

   Note: Complete this task by using IMM or a physical keyboard to prevent connection and lockout issues. If you're used to editing network configuration files in Linux®, you can use SSH and the `screen` command. Using a direct SSH session with `systemctl restart network` results in the loss of network connectivity and causes issues with the address change and service restart.

   a) Use IMM for remote access, or the local Console keyboard, to log in to the command line of the old appliance as the root user.

   b) Verify which network interface is the management interface by typing the following command:

   ```
   cat /etc/management_interface
   ```

   The interface that is listed in this file is the QRadar management interface.

   c) Change the directory to `/etc/sysconfig/network-scripts/`.

   d) Open the `ifcfg-<name>` file that was listed in the `/etc/management_interface` file.

   e) Change the IP address to an unused or decommissioned range by editing the IPADDR= line.

   f) Save the changes to the file.

   g) Restart networking by typing the following command:

   ```
   systemctl restart network
   ```

   Tip: After the network services are restarted, the IP address switch and the IP address change are completed, freeing up the old IP address to use on the new Console. If any QRadar processes on the system result in errors, QRadar operates normally if you switch the IP address back later. Don't unrack the old hardware until after you transfer the data to the new appliance.

4. Set IP addresses on the new QRadar Console:

   a) Use IMM for remote access or the local Console keyboard to log in to the command line of the new appliance as the root user.

   b) Change the IP address by typing the following command:

   ```
   /opt/qradar/bin/qchange_netsetup
   ```

   c) Use the Configuration Wizard to change the IP address of the system to the old Console's IP address.

   d) Save and exit the wizard to complete the address change.

   The new Console is installed with the old Console's IP address.

5. Copy certificates and custom-generated key pairs from the old appliance to the new appliance to ensure that log sources and scanners can connect to remote sources. You must also migrate any custom-generated private keys that you have by transferring the `/etc/ssh` and `/root/.ssh` directories.

   a) Log in to the old QRadar Console as the root user.

   b) Copy the data from the old hardware to the new appliance by using the **`rsync`** as in the following examples:

   Tip: For better performance when you use a crossover cable solution, use rsync -av instead of rsync -avz.

   Use this example for certificates:

```
Example: rsync -avz /opt/qradar/conf/trusted_certificates/
   root@new_appliance:/opt/qradar/conf/trusted_certificates/
```

Use these examples for SSH:

```
Example 1: rsync -avz /etc/ssh/ root@new_appliance:/etc/ssh
```

```
Example 2: rsync -avz /root/.ssh/ root@new_appliance:/root/.ssh
```

c) Wait for the transfer to complete.

d) If you are using custom SSL certificates, follow these steps:

i) Copy the certificate or intermediate certificate from the `/etc/httpd/conf/certs` directory on the old Console to the `/tmp` directory or your preferred location on the new Console.

Do not copy the certificate to the `/etc/httpd/conf/certs` directory on a new Console.

ii) Install the SSL certificate that you copied on the new Console by using `/opt/qradar/bin/install-ssl-cert.sh -i` and follow the instructions.

The wizard prompts you for a private key. You might have to copy the private key to the server if it is not stored in the `/etc/httpd/conf/certs/` directory. It is usually a best practice not to store the private key on the server itself.

Important: If the Console on your new appliance has a different certificate authority (CA) certificate than the Console on your old appliance, the CA from your old appliance should be placed under the directory `/etc/pki/ca-trust/source/anchors` and run the command $ `update-ca-trust`.

Warning:

- Verify that when your migration completes, the certificates on the console in /etc/http/conf/certs match that of the managed hosts
- Do not copy the certificate key (cert.key) from the console to the MH.

The required certificate and ssh key files are transferred to the new Console. You can now migrate event and flow data from the old Console to the new Console.

6. Restore the backup configuration to the new QRadar Console appliance:

a) Using **SCP**, copy the configuration backup file that you downloaded previously to the `/store/backupHost/inbound/` directory on the new Console.

b) Log in to the new QRadar Console as an administrator.

c) Click the **Admin** tab and select the **Backup and Recovery** icon.

d) Select the configuration backup that you copied to the Console and click **Restore**.

e) In the restore options list, check **Select All Configuration Items** and **Select All Data Items**.

f) Click **Restore** to start the configuration restore process.

Note: The restore process might take a while to complete.

g) After the restore process is complete, log in to QRadar.

h) From the **Admin** tab, click **Advanced** > **Deploy Full Configuration**.

i) Verify that event or flow sources that reported to the original host are now processed in QRadar.

After the host is added back to the QRadar deployment, the deployment process ensures that the required configuration is regenerated on the new appliance. Verify that log source data is pulled and that flow data is received by the new Console. Any log sources that are not collecting data might require certificates to be moved to the new host.

When the configuration is finished restoring on the new console, you might receive an error that indicates that the console license keys expired. You can add the new licenses to resolve this error.

7. Transfer any event and flow data to the new hardware.

   The data transfer can be a lengthy process. You can use cross-over cables to quicken the transfer of event and flow information if your appliances are located in the same data center. Data is moved in one month intervals to keep the performance impact at a minimum. The `syncAriel.sh` utility does not move certificates or configurations, only data that is stored in the `/store/ariel/` directory. SSH traffic must be allowed to migrate the data. You might be required to accept SSH keys and provide the root password for the target server to start the transfer.

   a) Download `syncAriel.sh` from step 7 in this technote (http://www-01.ibm.com/support/docview.wss?uid=swg21984607).

   b) Log in to the old QRadar Console as the root user.

   c) Using **SCP**, copy the `syncAriel.sh` utility to the old Console.

   d) Navigate to the directory with the `syncAriel.sh` utility and type the following command:

   ```
   chmod +x syncAriel.sh
   ```

   e) Type the following command:

   ```
   screen
   ```

   Note: For data transfers, start a screen session to reestablish the connection in case of a minor network outage. To detach the session so that you can log out, type **Ctrl+A** and press **D** or use **Ctrl+D**, then type **Ctrl+D** and use **`screen -r`** to reattach to the screen session.

   f) Run the utility by typing the following command:

   ```
   sh syncAriel.sh -i <new_Console's_IPAddress>
   ```

   g) Wait for the transfer to complete, then close the **`screen`** session.

   Data is migrated from the `/store/ariel` directory of the old Console to the new Console.

   If your connection dropped or a network outage occurred, you can run the `syncAriel.sh` utility again to migrate data. The `syncAriel.sh` utility keeps track of files that have been rsync'd to the new appliance and data that has already been transferred is not copied a second time.

   If the transfer fails or encounters errors, transfer the data manually by using SCP, SFTP, or another file transfer method.

8. Optional: Copy over event collector data, if you have any data in `/store/ec`.

   a) Log in to the old appliance as the root user.

   b) Stop ecs-ec-ingress on the old appliance by typing the following command:

   ```
   systemctl stop ecs-ec-ingress
   ```

   c) Log in to the new appliance as the root user.

   d) Create a file on the new appliance to prevent ecs-ec-ingress from automatically restarting by typing the following command:

   ```
   touch /storetmp/ecs-ec-ingress.ecs-ec-ingress.manually_stopped
   ```

   e) Stop ecs-ec-ingress on the new appliance by typing the following command:

   ```
   systemctl stop ecs-ec-ingress
   ```

   f) Copy the data from `/store/ec` on the old appliance to `/store/ec` on the new appliance.

   g) Remove the file that is created in substep d from the new appliance by typing the following command:

```
rm -f /storetmp/ecs-ec-ingress.ecs-ec-ingress.manually_stopped
```

h) Start ecs-ec-ingress on the new appliance by typing the following command:

```
systemctl start ecs-ec-ingress
```

Results

After the data transfer is complete, you might want to keep the old Console on hand in case you need to revert to the old appliance. Otherwise, after a week or two, you won't need the old Console and you can decommission or repurpose it for other uses.

Replacing a QRadar Console with an appliance that uses a new IP address

Migrate data from an older QRadar Console to a new Console appliance that uses a new IP address. All managed host appliances stay as-is. Use this process for non-HA appliances.

Before you begin

You must complete a QRadar installation on the new Console with a matching software version to the old Console.

About this task

You don't have to remove managed hosts from the old QRadar Console because the new QRadar Console takes over any existing hosts in the deployment. This procedure allows managed hosts in the deployment to continue to receive events while the Console is offline.

Important: App data is separated from the configuration backup and restore. To backup and restore app data, see Backing up and restoring app data.

Procedure

1. Prepare your new hardware:
   a) Rack the appliance and connect network connections.
   b) Review the paperwork for your appliance to determine which QRadar version is installed on the new hardware.
2. Review your software version.
   a) If your Console software version is older than the software on the appliance, reinstall the appliance with the newest ISO that is less than or equal to the Console software version. Download the ISO file from Fix Central (www.ibm.com/support/fixcentral/).
   b) Follow the installation wizard to complete the installation.
   c) Type a root password for the appliance.
   d) Type a new IP address and network information for the new hardware.
   e) Log in as a root user and select the appliance type during the installation process.
   f) If your Console patch version is newer than the software on the appliance, download and install the SFS (software fix/patch) from Fix Central (www.ibm.com/support/fixcentral/).
3. On the navigation menu (☰), click **Admin**.
4. In the **System Configuration** section, click **Backup and Recovery**.
5. Select the archive that you want to restore, and click **Restore**.
6. On the **Restore a Backup** window, configure the following parameters and then click **Restore**.

*Table 1. **Restore a Backup** parameters*	
Parameter	**Description**
Select All Configuration Items	Indicates that all configuration items are included in the restoration of the backup archive. This checkbox is selected by default.
Restore Configuration	Lists the configuration items to include in the restoration of the backup archive. All items are selected by default.
Select All Data Items	Indicates that all data items are included in the restoration of the backup archive. This checkbox is selected by default.
Restore Data	Lists the configuration items to include in the restoration of the backup archive. All items are cleared by default.

7. Stop the IP table service on each managed host in your deployment. The IP tables is a Linux-based firewall.
   a) Using SSH, log in to the managed host as the root user.
   b) For App Host, type the following commands:
      systemctl stop docker_iptables_monitor.timer
      systemctl stop iptables
   c) For all other managed hosts, type the following command:
      systemctl stop iptables
   d) Repeat for all managed hosts in your deployment.
8. On the **Restore a Backup** window, click **Test Hosts Access**.
9. After testing is complete for all managed hosts, verify that the status in the **Access Status** column indicates a status of **OK**.
10. If the **Access Status** column indicates a status of **No Access** for a host, stop iptables again, and then click **Test Host Access** again to attempt a connection.
11. On the **Restore a Backup** window, configure the parameters.

    Important: By selecting the **Installed Applications Configuration** checkbox, you restore the install app configurations only. Extension configurations are not restored. Select the **Deployment Configuration** checkbox if you want to restore extension configurations.
12. Click **Restore**.
13. Click **OK**.
14. Click **OK** to log in.
15. Choose one of the following options:
    - If the user interface was closed during the user restore process, open a web browser and log in to QRadar.
    - If the interface was not closed, the login window is displayed. Log in to QRadar.
16. View the results of the restore process and follow the instructions to resolve any errors.
17. Refresh your web browser window.
18. From the **Admin** tab, select **Advanced** > **Deploy Full Configuration**.

    QRadar continues to collect events when you deploy the full configuration. When the event collection service must restart, QRadar does not restart it automatically. A message displays that gives you the option to cancel the deployment and restart the service at a more convenient time.
19. To enable the IP tables for an App Host, type the following command:

```
systemctl start docker_iptables_monitor.timer
```

What to do next

After the data transfer is complete, you might want to keep the old Console on hand in case you need to revert to the old appliance. Otherwise, after a week or two, the old Console is no longer required and can be decommissioned or repurposed for other uses.

To verify that your migration is successful, log in as an administrator, click the **Log Activity** tab and perform a search to see whether events are flowing. Then, click the **Network Activity** tab and perform a search to see whether flows are being processed.

Chapter 2. QRadar M6 appliance overview

The M6 appliances are the latest generation of appliances for IBM QRadar. You can configure the M6 appliances by using either the Lenovo System SR630 or SR650, or by using the Dell R740xd XL and designated with a -C, such as the QRadar Network Insights 1940-C.

After you install a QRadar appliance, you must apply your license keys. For more information, see License keys.

IBM QRadar appliances are certified to support a certain maximum events per second (EPS) rate. Maximum EPS depends on the type of data that is processed, system configuration, and system load. For more information, see QRadar maximum EPS certification methodology.

Update the firmware on QRadar appliances to take advantage of additional features and updates for the internal hardware components. For more information, see Firmware updates and QRadar M6 Firmware Update Procedure.

Management controller

The IBM QRadar appliances use a management controller for systems-management functions.

IBM QRadar appliances contain an integrated service processor, which provides advanced service-processor control, monitoring, and alerting functions and consolidates the service processor functionality, super I/O, video controller, and remote presence capabilities into a single chip on the server system board.

For more information about the Lenovo management controller, see Lenovo XClarity Controller(https://sysmgt.lenovofiles.com/help/index.jsp?topic=%2Fcom.lenovo.systems.management.xcc.doc%2Fdw1lm_c_ch1_introduction.html).

For more information about the Dell management controller, see Dell iDRAC Controller (https://www.delltechnologies.com/en-us/solutions/openmanage/idrac.htm).

For instructions on how to configure the Lenovo management controller, see XClarity Controller User Guide (https://sysmgt.lenovofiles.com/help/topic/com.lenovo.systems.management.xcc.doc/xcc_book.pdf.

For instructions on how to configure the Dell management controller, see iDRAC Controller User Guide (https://www.dell.com/support/article/en-ca/sln306877/dell-poweredge-how-to-configure-the-idrac9-and-the-lifecycle-controller-network-ip?lang=en).

QRadar xx05

Use the IBM QRadar xx05 (MTM 4563-Q3E) appliance for various appliance types in your deployment. QRadar xx05 is based on the Lenovo System SR630 M6.

The QRadar xx05 supports the following appliance types:

- QRadar Event Processor 1605
- QRadar Flow Processor 1705
- QRadar 1805 Event and Flow processor
- QRadar 3105 (All-in-One)
- QRadar 3105 (Console)
- QRadar Log Manager 1605
- QRadar Risk Manager
- QRadar Vulnerability Manager
- QRadar Log Manager 3105 (All-in-One)

- QRadar Log Manager 3105 Console
- QRadar App Host
- QRadar Data Node 1405

The following table describes hardware information and requirements for the QRadar xx05 appliance:

Table 2. QRadar xx05 specifications

Description	**Value**
Maximum capacity	QRadar Event Processor 1605: 20,000 EPS QRadar Flow Processor 1705: 1,200,000 FPM QRadar 1805 Event and Flow processor: 5000 EPS, 200,000 FPM QRadar 3105 (All-in-One): 5000 EPS, 200,000 FPM
CPU	2 x Xeon Silver 4210 10C 2.1 GHz 85W
Network management transceivers	2 x 10 GbE Short Range SFP+ The transceivers might have one of the following part numbers: • Avago AFBR-709SMZ-IB8 • Finisar FTLX8571D3BCL-BN • BNT BN-CKM-SP-SR Use these transceivers with the 2 x 10 GbE SFP+ ports, labeled as [3] in the appliance diagram
Ports	4 x 1 Gb Ethernet ports 2 x 10 GbE SFP+ ports 1 x RJ-45 10/100/1000 Mb Ethernet systems management (IMM) port 2 x 16 Gbps Fibre Channel SFP+ ports
Memory	64 GB (4 x 16 GB)
Storage	10 x 1.2 TB 7.2 K 12 Gbps 2.5" NL SAS 930-16i 4 Gb / RAID 6 QRadar 3105: 6 TB available to store event and flow data All other xx05 appliances: 8 TB available to store event and flow data
Power® supply	Dual redundant 750 W AC power supply
Dimensions	28.1 inches deep x 17.1 inches wide x 1.7 inches high
Included components	Event Collector Event processor for processing events Internal storage for events QRadar Data Node appliance

The following image is of the QRadar xx05 appliance.

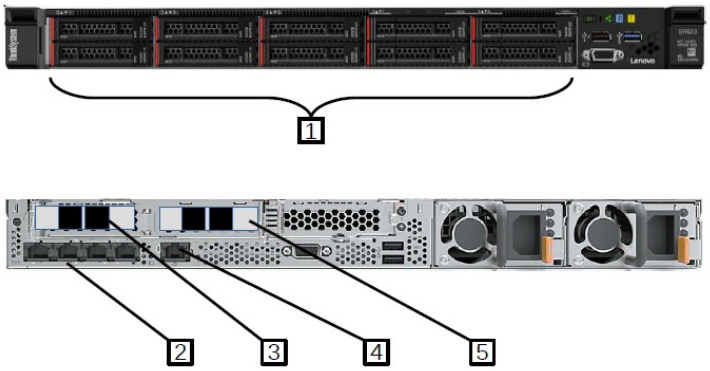


Figure 1. Front and rear panel of the QRadar xx05 appliance.

Table 3. Legend for use with the QRadar xx05 image	
Label	**Description**
1	Event data storage
2	Management ports (1 GbE TX)
3	Management ports (10 GbE SFP+)
4	1x RJ-45 10/100/1000 Mb Ethernet systems management (IMM) port
5	Fibre Channel ports (16 Gb SFP+)

You can upgrade your license to migrate your QRadar Log Manager 3105 (All-in-One) to QRadar 3105 (All-in-One). For more information, see *QRadar Log Manager to QRadar SIEM Migration Guide*.

For information about battery removal, see Removing the coin-cell battery (https://thinksystem.lenovofiles.com/help/index.jsp?topic=%2F7X01%2Fcoincell_battery_replacement.html&cp=4_6_8_12).

QRadar xx29

The IBM QRadar xx29 (MTM 4563-Q4A) appliance supports various appliance types in your deployment. QRadar xx29 is based on the Lenovo System SR650 M6.

The QRadar xx29 supports the following appliance types:

- QRadar Event Processor 1629
- QRadar Flow Processor 1729
- QRadar Event and Flow Processor 1829
- QRadar 3129 (All-in-One)
- QRadar 3129 (Console)
- QRadar App Host
- QRadar Data Node 1429

The following table describes hardware information and requirements for the QRadar xx29 appliance:

Table 4. QRadar xx29 specifications	
Description	**Value**
Maximum capacity	QRadar Event Processor 1629: 40,000 EPS QRadar Flow Processor 1729: 2,400,000 FPM QRadar Event and Flow Processor 1829: 15,000 EPS, 300,000 FPM QRadar 3129 (All-in-One): 15,000 EPS, 300,000 FPM
CPU	2 x Xeon Silver 4214 12C 2.2 GHz 85W
Network management transceivers	2 x 10 GbE Short Range SFP+ The transceivers might have one of the following part numbers: • Avago AFBR-709SMZ-IB8 • Finisar FTLX8571D3BCL-BN • BNT BN-CKM-SP-SR Use these transceivers with the 2 x 10 GbE SFP+ ports, labeled as [4] in the appliance diagram
Ports	4 x 1 Gb Ethernet ports 2 x 10 GbE SFP+ ports 1 x RJ-45 10/100/1000 Mb Ethernet systems management (IMM) port 2 x 16 Gbps Fibre Channel SFP+ ports
Memory	8 x 32 GB (256 GB)
Storage	12 x 8 TB 7.2 K 12 Gbps NL SAS 930-16i 4 GB / RAID 6 3129: 64 TB available to store event and flow data All other xx29 appliances: 77 TB available to store event and flow data
Power supply	Dual Redundant 750 W AC
Dimensions	28.3 inches deep x 17.5 inches wide x 3.4 inches high
Included components	Event Collector Event processor for processing events and flows Internal storage for events and flows QRadar Data Node appliance

The following image is of the QRadar xx29 appliance.

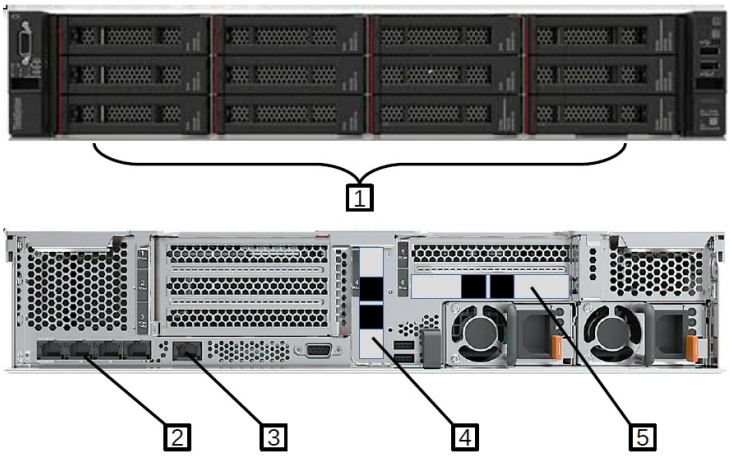


Figure 2. Front and rear panel of the QRadar xx29 appliance

Table 5. Legend for use with the QRadar xx29 image	
Label	**Description**
1	Event data storage
2	Management ports (1 GbE TX)
3	1 x RJ-45 10/100/1000 Mb Ethernet systems management (IMM) port
4	Management ports (10 GbE SFP+)
5	Fibre Channel ports (16 Gb SFP+)

For information about battery removal, see Removing the coin-cell battery (https://thinksystem.lenovofiles.com/help/index.jsp?topic=%2F7X05%2Fcmos_battery_replacement.html&cp=4_8_8_13&anchor=CMOS_battery_replacement).

QRadar xx48

The IBM QRadar xx48 (MTM 4563-Q5B) appliance captures logs from sources that generate a large amount of traffic without a need for load balancing. QRadar xx48 is based on the Lenovo System SR630 M6.

The QRadar xx48 appliance handles the higher levels of performance that are required by enterprise class clients. For example, you can use the QRadar xx48 appliance for the following requirements:

- You want faster processing to search and analyze a large amount of data.
- You want to reduce the footprint of an IBM QRadar deployment, so you install QRadar xx48 appliances to reduce rack space.

The QRadar xx48 supports the following appliance types:

- QRadar Event Processor 1648
- QRadar Flow Processor 1748
- QRadar Event and Flow Processor 1848
- QRadar 3148 (All-in-One)
- QRadar 3148 (Console)
- QRadar App Host
- QRadar Data Node 1448

The following table describes hardware information and requirements for the QRadar xx48 appliance:

Table 6. QRadar xx48 specifications

Description	Value
Maximum capacity	QRadar Event Processor 1648: 80,000 EPS QRadar Flow Processor 1748: 3,600,000 FPM QRadar Event and Flow Processor 1848: 30,000 EPS, 1,200,000 FPM QRadar 3148 (All-in-One): 30,000 EPS, 1,200,000 FPM
CPU	2 x Xeon Gold 6230 20C 2.10 GHz 22 MB Cache 125W
Network management transceivers	2 x 10 GbE Short Range SFP+ The transceivers might have one of the following part numbers: • Avago AFBR-709SMZ-IB8 • Finisar FTLX8571D3BCL-BN • BNT BN-CKM-SP-SR Use these transceivers with the 2 x 10 GbE SFP+ ports, labeled as [3] in the appliance diagram
Ports	4 x 1 Gb Ethernet ports 2 x 10 GbE SFP+ ports 1 x RJ-45 10/100/1000 Mb Ethernet systems management (IMM) port 2 x 16 Gbps Fibre Channel SFP+ ports
Memory	8 x 32 GB (256 GB)
Storage	6 x 3.84 TB 2.5" SAS SSD, 930-8i RAID 6 QRadar 3148: 13 TB available to store event and flow data All other xx48 appliances: 15 TB available to store event and flow data
Dimensions	29.5 inches deep x 17.1 inches wide x 1.7 inches high
Power supply	Dual redundant 750 W AC

The following image is of the QRadar xx48 appliance.

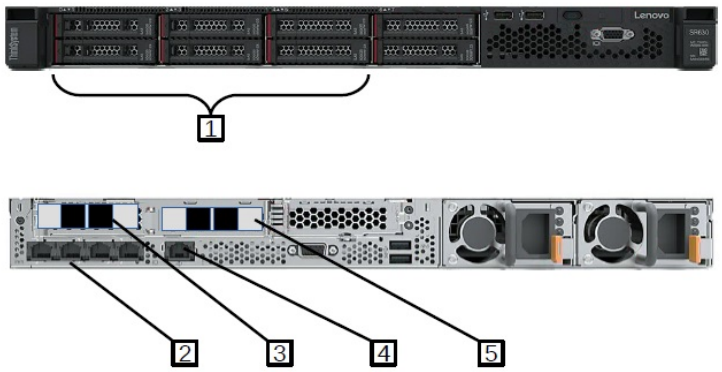


Figure 3. Front and rear panel of the QRadar xx48 appliance

Table 7. Legend for use with the QRadar xx48 image	
Label	**Description**
1	Event data storage
2	Management ports (1 GbE TX)
3	Management ports (10 GbE SFP+)
4	1 x RJ-45 10/100/1000 Mb Ethernet systems management (IMM) port
5	Fibre Channel ports (16 Gb SFP+)

For information about battery removal, see
Removing the coin-cell battery (https://thinksystem.lenovofiles.com/help/index.jsp?topic=%2F7X01%2Fcoincell_battery_replacement.html&cp=4_6_8_12).

QRadar Network Insights 1901

The IBM QRadar Network Insights 1901 (MTM 4563-F8Y) appliance provides detailed analysis of network flows to extend the threat detection capabilities of IBM QRadar. QRadar Network Insights 1901 is based on the Lenovo System SR630 M6.

With four 1G capture ports on a Napatech card, the QRadar Network Insights 1901 appliance provides the same capabilities as the QRadar Network Insights 1920 appliance but on a lower-price hardware platform that is designed for 1 Gbps network connectivity.

The QRadar Network Insights 1901 appliance has the following hardware specifications:

Table 8. QRadar Network Insights 1901 specifications	
Hardware	**Description**
CPU	1 x Xeon Gold 6240 18C 2.6GHz 24MB Cache 150W
Network capture transceivers	4 x 1 GbE TX RJ-45 Transceiver Avago ABCU-5710RZ or ABCU-5740RZ 4 x 1 G SX MMF Transceiver (P/N: D10E5LL) Avago AFBR-5715PZ Use these transceivers with ports, labeled as [5] in the appliance diagram
Network management transceivers	2 x 10 GbE Short Range SFP+ The transceivers might have one of the following part numbers: • Avago AFBR-709SMZ-IB8 • Finisar FTLX8571D3BCL-BN • BNT BN-CKM-SP-SR Use these transceivers with the 2 x 10 GbE SFP+ ports, labeled as [3] in the appliance diagram
Ports	4 x 1 Gb Ethernet ports 2 x 10 GbE SFP+ ports 1 x RJ-45 10/100/1000 Mb Ethernet systems management (IMM) port 4 x Network capture (SFP+) ports
Storage	2 x 480GB Enterprise Performance SATA 2.5” SSD / 530-8i / RAID 1
Memory	4 x 32 GB (128 GB)
Traffic	1 Gbps

Table 8. QRadar Network Insights 1901 specifications (continued)	
Hardware	**Description**
Power supply	Dual redundant 750 W AC
Dimensions	28.1 inches deep x 17.1 inches wide x 1.7 inches high

System performance of QRadar Network Insights appliances varies depending on the exact configuration and tuning of the system components. It is influenced not only by hardware, but also factors such as search, extraction criteria, and the amount of network data.

For more information, see Performance impacts in the IBM QRadar Network Insights *Installation Guide*.

The following image is of the QRadar Network Insights 1901 appliance.

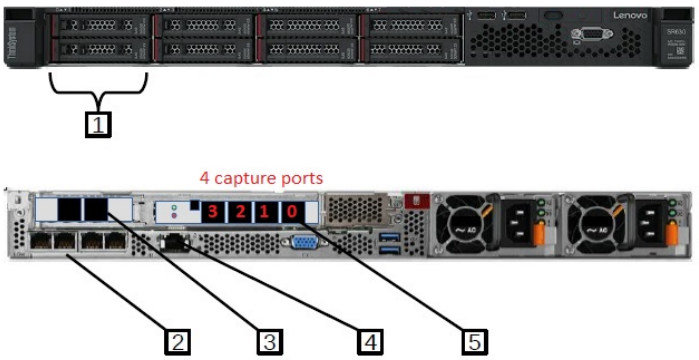


Figure 4. Front and rear panel of the QRadar Network Insights 1901 appliance

Table 9. Legend for use with the QRadar Network Insights 1901 image	
Label	**Description**
1	QRadar Firmware Storage
2	Management ports (1 GbE TX)
3	Management ports (10 GbE SFP+)
4	1x RJ-45 10/100/1000 Mb Ethernet systems management (IMM) port
5	Network Packet Capture (SFP+)

Note: Only the Network Packet Capture card [5] can be used for capturing network packet data.

For information about battery removal, see
Removing the coin-cell battery (https://thinksystem.lenovofiles.com/help/index.jsp?topic=%2F7X01%2Fcoincell_battery_replacement.html&cp=4_6_8_12).

QRadar Network Insights 1910

The IBM QRadar Network Insights 1910 (MTM 4563-F7Y) appliance offers 1 Gbps and 10 Gbps connectivity in a smaller, lower-cost appliance for deployments that require 10 Gbps connectivity but don't require the same level of processing or performance that is found in the more powerful 1920 appliance. QRadar Network Insights 1910 is based on the Lenovo System SR630 M6.

Table 10. QRadar Network Insights 1910 specifications	
Description	**Value**
CPU	1 x Xeon Gold 6240 18C 2.6 GHz 24 MB Cache 150W

Table 10. QRadar Network Insights 1910 specifications (continued)	
Description	**Value**
Network capture transceivers	• 4 x 10 Gb Short Range Fiber Transceivers (Avago AFBR-703SDZ or AFBR-709SMZ) • 4 x 10 Gb Long Range Fiber Transceivers (Avago AFCT-739SMZ) Use these transceivers with the 4 x Network Packet Capture (SFP+) ports, labeled as [5] in the appliance diagram
Network management transceivers	2 x 10 GbE Short Range SFP+ The transceiver may have one of the following part numbers: • Avago AFBR-709SMZ-IB8 • Finisar FTLX8571D3BCL-BN • BNT BN-CKM-SP-SR Use these transceivers with the 2 x 10 GbE SFP+ ports, labeled as [3] in the appliance diagram
Ports	2 x 10 GbE SFP+ ports 4 x Network capture (SFP+) ports 3 x 10/100/1000 Base-T network ports 1 x 10/100/1000 Base-T QRadar management port 1 x RJ-45 10/100/1000 Mb Ethernet systems management (IMM) port
Memory	4 x 32 GB (128 GB)
Storage / Hard disks	2 x 480 GB Enterprise Performance SATA 2.5” SSD / 530-8i / RAID 1
Traffic	10 Gbps
Power supply	Dual redundant 750 W AC
Physical dimensions	28.1 inches deep x 17.1 inches wide x 1.7 inches high

The following image is of the QRadar Network Insights 1910 appliance.

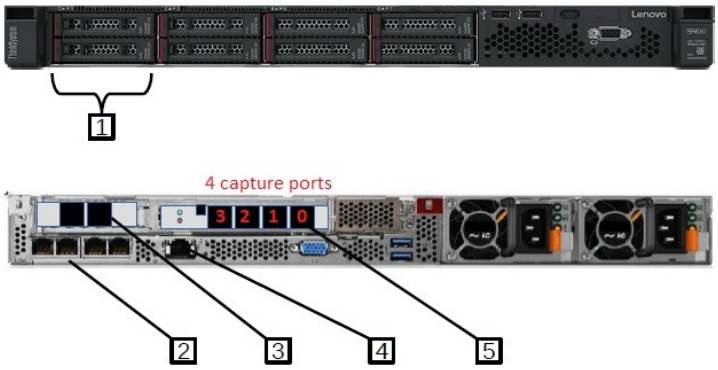


Figure 5. Front and rear panel of the QRadar Network Insights 1910 appliance

Table 11. Legend for use with the QRadar Network Insights 1910 image	
Label	**Description**
1	QRadar firmware storage
2	Management ports (1 GbE TX)
3	Management ports (10 GbE SFP+)
4	1x RJ-45 10/100/1000 Mb Ethernet systems management (IMM) port
5	Network Packet Capture (SFP+) ports

For information about battery removal, see
Removing the coin-cell battery (https://thinksystem.lenovofiles.com/help/index.jsp?topic=%2F7X01%2Fcoincell_battery_replacement.html&cp=4_6_8_12).

QRadar Network Insights 1920

The IBM QRadar Network Insights 1920 (MTM 4563-F5F) appliance provides detailed analysis of network flows to extend the threat detection capabilities of IBM QRadar. QRadar Network Insights 1920 is based on the Lenovo System SR650 M6.

The appliance has two Napatech cards, each with four ports. By default, the four ports on the first network capture card are configured for inbound traffic from the network tap. If the appliance is included in a stack, the ports are reconfigured for two inbound ports and two outbound ports.

The management ports are associated with port 4 and port 6. These are used to replicate data between QRadar Network Insights and the Console. Port 3 is reserved for the XClarity Controller (XCC), remote management system.

The only ports that accept raw network traffic through a mirrored span port or a network tap are the designated Napatech card ports. The Network Packet Capture Card is displayed in Figure 1. If it is a stand-alone QRadar Network Insights appliance, then all four ports are the same. If you are trying to stack the product, only two out of the four ports receive traffic.

For more information about cabling stacked appliances, see the QRadar Network Insights *Installation Guide*.

The second Napatech card is cabled internally for load balancing and cannot not be used. If you use these ports when you cable the appliance, you do not get any data.

The following table shows the hardware information and requirements for the IBM QRadar Network Insights 1920 (MTM 4563-F5F) appliance:

Table 12. QRadar Network Insights 1920 specifications	
Description	**Value**
Dimensions	28.3 inches deep x 17.5 inches wide x 3.4 inches high
CPU	2 x Xeon Gold 6240 18C 2.6 GHz 24 MB Cache 150W
Network capture transceivers	2 x 10 Gb Short Range fiber Transceivers (SFP+) (Avago AFBR-703SDZ or AFBR-709SMZ) 2 x 1 G TX RJ-45 Transceivers (SFP) (Avago ABCU-5710RZ or ABCU-5740RZ) 2 x 1 G SX LC Transceivers (SFP) (Avago AFBR-5715PZ) Use these transceivers with the network packet capture card, labeled as [5] in the appliance diagram.

Table 12. QRadar Network Insights 1920 specifications (continued)	
Description	**Value**
Network management transceivers	2 x 10 GbE Short Range SFP+ The transceivers can have one of the following part numbers: • Avago AFBR-709SMZ-IB8 • Finisar FTLX8571D3BCL-BN • BNT BN-CKM-SP-SR Use these transceivers with the 2 x 10 GbE SFP+ management ports, labeled as [2] in the appliance diagram.
Ports	2 x 10 GbE SFP+ ports 4 x Network capture ports (SFP/SFP+) (Model NT40E3-4) 4 x 1 Gb Ethernet ports 1 x RJ-45 10/100/1000 Mb Ethernet systems management (IMM) port
Storage	2 x 480 GB Enterprise Performance SATA 2.5” SSD / 530-8i / RAID 1
Memory	8 x 32 GB (256 GB)
Traffic	10 Gbps
Power supply	Dual redundant 750 W AC

System performance of QRadar Network Insights appliances varies depending on the exact configuration and tuning of the system components. It is influenced not only by hardware, but also factors such as the search, extraction criteria, and the amount of network data.

For more information, see Performance impacts in the IBM QRadar Network Insights *Installation Guide*.

The following image is of the QRadar Network Insights 1920 appliance.

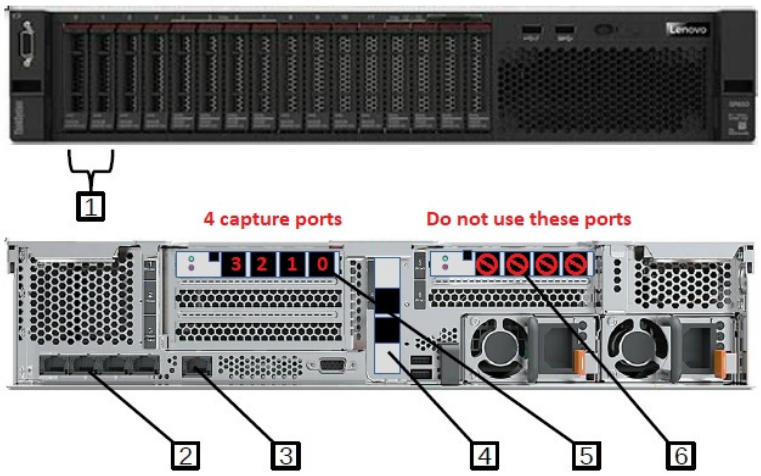


Figure 6. Front and back panel of the QRadar Network Insights 1920 appliance

Table 13. Legend for use with the QRadar Network Insights 1920 image	
Label	**Description**
1	QRadar Firmware Storage

Table 13. Legend for use with the QRadar Network Insights 1920 image (continued)	
Label	**Description**
2	Management ports (1 GbE TX)
3	1x RJ-45 10/100/1000 Mb Ethernet systems management (IMM) port
4	Management ports (10 GbE SFP+)
5	Network Packet Capture (SFP/SFP+)
6	Network Packet Capture (Unpopulated)

For information about battery removal, see Removing the coin-cell battery (https://thinksystem.lenovofiles.com/help/index.jsp?topic=%2F7X05%2Fcmos_battery_replacement.html&cp=4_8_8_13&anchor=CMOS_battery_replacement).

QRadar Network Insights 1920-C

The IBM QRadar Network Insights 1920-C (MTM 4654-F4F) appliance provides detailed analysis of network flows to extend the threat detection capabilities of IBM QRadar.

The appliance has two Napatech cards, each with four ports. By default, the four ports on the first network capture card are configured for inbound traffic from the network tap. If the appliance is included in a stack, the ports are reconfigured for 2 inbound and 2 outbound. For more information about cabling stacked appliances, see the IBM QRadar Network Insights *Installation Guide*.

The second Napatech card is cabled internally for load balancing and cannot not be used. If you use these ports when you cable the appliance, you do not get any data.

The following table shows the hardware information and requirements for the IBM QRadar Network Insights 1920-C (MTM 4654-F4F) appliance.

Table 14. QRadar Network Insights 1920-C specifications	
Description	**Value**
CPU	2 x Xeon Gold 6132 14C 2.6 GHz 19 MB Cache 3.70 GHz 140 W
Network capture transceivers	2 x 10 Gb Short Range fiber Transceivers (Avago AFBR-703SDZ or AFBR-709SMZ) 2 x 1 G TX RJ-45 Transceivers (Avago ABCU-5710RZ or ABCU-5740RZ) 2 x 1 G SX LC Transceivers (Avago AFBR-5715PZ) Use these transceivers with the network packet capture card, labeled as [2] in the appliance diagram.
Network management transceivers	2 x 10 GbE Short Range SFP+ The transceivers can have one of the following part numbers: • Avago AFBR-709SMZ-IB8 • Finisar FTLX8571D3BCL-BN • BNT BN-CKM-SP-SR Use these transceivers with the 2 x 10 GbE SFP+ ports, labeled as [3] in the appliance diagram.

Table 14. QRadar Network Insights 1920-C specifications (continued)	
Description	**Value**
Ports	Network Packet Capture (SFP/SFP+) port (Model NT40E3-4) 4 x 1 Gb Ethernet ports 1 x RJ-45 10/100/1000 Mb Ethernet systems management (IMM) port 2 x 10 Gbps SFP+ management ports
Memory	128 GB, 8 x 16 GB
Storage	2 x 240 GB SATA 2.5" SSD, 240 GB Total (RAID1)
Traffic rate	10 Gbps
Power supply	Dual redundant 750 W AC
Unit weight	73 lbs
Physical dimensions	29.0 inches deep x 17.1 inches wide x 3.4 inches high

The following image is of the QRadar Network Insights 1920-C appliance.

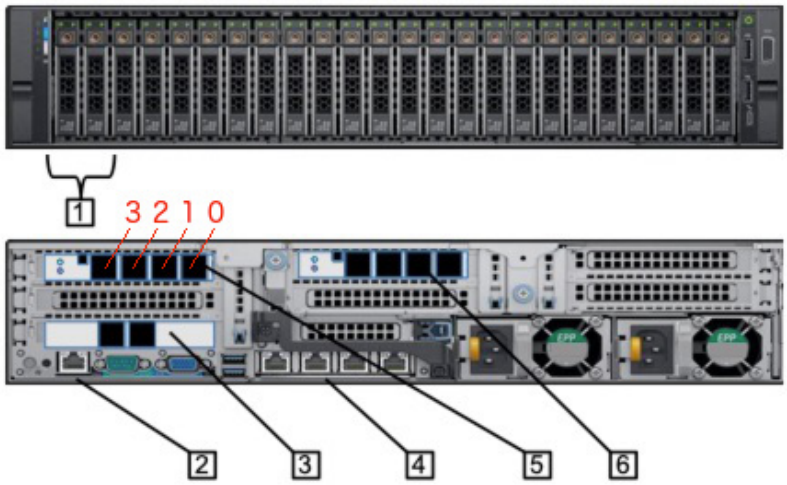


Figure 7. Front and back panel of the QRadar Network Insights 1920-C appliance

Table 15. Legend for use with the QRadar Network Insights 1920-C image	
Label	**Description**
1	QRadar firmware storage
2	1 x RJ-45 10/100/1000 Mb Ethernet systems management (IMM) port
3	Management ports (10 GbE SFP+)
4	Management ports (1 GbE TX)
5	Network Packet Capture (SFP/SFP+) Ports are numbered 3, 2, 1, 0, from left to right.
6	Do not use these ports

For information about battery replacement, see *Dell EMC PowerEdge R740 Installation and Service Manual* (https://topics-cdn.dell.com/pdf/poweredge-r740_owners-manual_en-us.pdf).

QRadar Network Insights 1940

New in 7.4.1 The IBM QRadar Network Insights 1940 (MTM 4563-F6G) appliance provides detailed analysis of network flows to extend the threat detection capabilities of IBM QRadar. QRadar Network Insights 1940 is based on the Lenovo System SR650.

The appliance has two Napatech 40 GbE cards. By default, the two ports on the first network capture card are configured for inbound traffic from a network tap or mirrored span. If the appliance is included in a stack, the ports are reconfigured for one inbound and one outbound.

The second Napatech card is cabled internally for load balancing and cannot not be used. The QSFP+ ports on this card are disabled. These ports will not receive data if they are connected to external traffic sources.

The management ports are associated with port items 2 and 4 in the diagram. These are used to replicate data between QRadar Network Insights and the Console. The port item 3 is reserved for the management controller remote management system.

For more information about cabling stacked appliances, see the QRadar Network Insights *Installation Guide*.

The following table shows the hardware information and requirements for the IBM QRadar Network Insights 1940 (MTM 4563-F6G) appliance:

Table 16. QRadar Network Insights 1940 specifications

Description	**Value**
CPU	2 x Xeon Gold 6240 18C 2.6GHz 24MB Cache 150W
Network capture transceivers	2 x 40 GbE SR4 QSFP+ transceivers (Finisar FTL410QD2C) Use these transceivers with the network packet capture card, labeled as [5] in the appliance diagram.
Network management transceivers	2 x 10 GbE Short Range SFP+ The cards may have one of the following part numbers: • Avago AFBR-709SMZ-IB8 • Finisar FTLX8571D3BCL-BN • BNT BN-CKM-SP-SR Use these cards with the 2 x 10 GbE SFP+ management ports, labeled as [4] in the appliance diagram.
Ports	4 x 1 Gb Ethernet ports 2 x 10 GbE SFP+ ports 1 x RJ-45 10/100/1000 Mb Ethernet systems management (IMM) port 2 x 40 GbE Network capture ports (QSFP+) (Model NT200A02)
Storage	2 x 480 GB Enterprise Performance SATA 2.5” SSD / 530-8i / RAID 1
Memory	8 x 32 GB (256 GB)
Traffic	10 Gbps
Power supply	Dual redundant 750 W AC

Table 16. QRadar Network Insights 1940 specifications (continued)	
Description	**Value**
Dimensions	28.3 inches deep x 17.5 inches wide x 3.4 inches high

System performance of QRadar Network Insights appliances varies depending on the on Inspection settings and the type and amount of network data.

For more information, see Performance impacts in the IBM QRadar Network Insights *Installation Guide*.

The following image is of the QRadar Network Insights 1940 appliance.

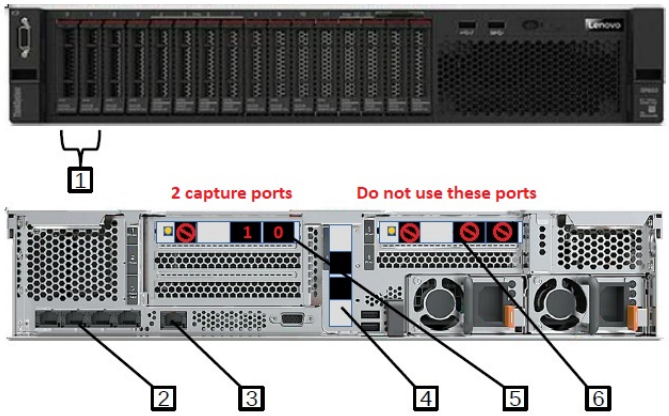


Figure 8. Front and back panel of the QRadar Network Insights 1940 appliance

Table 17. Legend for use with the QRadar Network Insights 1940 image	
Label	**Description**
1	QRadar system storage
2	Management ports (1 GbE TX)
3	1 x RJ-45 10/100/1000 Mb Ethernet systems management port
4	Management ports (10 GbE SFP+)
5	2 x 40 GbE Network capture ports (QSFP+)
6	Network packet capture (Unpopulated)

For information about battery removal, see Removing the coin-cell battery (https://thinksystem.lenovofiles.com/help/index.jsp?topic=%2F7X05%2Fcmos_battery_replacement.html&cp=4_8_8_13&anchor=CMOS_battery_replacement).

QRadar Network Insights 1940-C

New in 7.4.1 The IBM QRadar Network Insights 1940-C (MTM 4654-F7G) appliance provides detailed analysis of network flows to extend the threat detection capabilities of IBM QRadar. QRadar Network Insights 1940-C is based on the Dell R740xd XL server.

The appliance has two Napatech 40 GbE cards. By default, the two ports on the first network capture card are configured for inbound traffic from a network tap or mirrored span. If the appliance is included in a stack, the ports are reconfigured for one inbound and one outbound.

The second Napatech card is cabled internally for load balancing and cannot not be used. The QSFP+ ports on this card are disabled. These ports will not receive data if they are connected to external traffic sources.

The management ports are associated with port items 3 and 4 in the diagram. These are used to replicate data between QRadar Network Insights and the Console. The port item 2 is reserved for the management controller remote management system.

For more information about cabling stacked appliances, see the QRadar Network Insights *Installation Guide*.

The following table shows the hardware information and requirements for the IBM QRadar Network Insights 1940-C (MTM 4654-F7G) appliance:

Table 18. QRadar Network Insights 1940-C specifications

Description	**Value**
CPU	2 x Xeon Gold 6240 20C 2.6 GHz 24 MB Cache 150W
Network capture transceivers	2 x 40 GbE SR4 QSFP+ transceivers (Finisar FTL410QD2C) Use these transceivers with the network packet capture card, labeled as [5] in the appliance diagram.
Network management transceivers	2 x 10 GbE Short Range SFP+ The cards may have one of the following part numbers: • Avago AFBR-709SMZ-IB8 • Finisar FTLX8571D3BCL-BN • BNT BN-CKM-SP-SR Use these cards with the 2 x 10 GbE SFP+ management ports, labeled as [3] in the appliance diagram.
Ports	4 x 1 Gb Ethernet ports 2 x 10 GbE SFP+ ports 1 x RJ-45 10/100/1000 Mb Ethernet systems management (IMM) port 2 x Network capture ports (QSFP+) (Model NT200A02)
Storage	2 x 480 GB SATA 2.5” SSD PERC H730P RAID 1
Memory	8 x 32 GB (256 GB)
Traffic	10 Gbps
Power supply	Dual redundant 750 W AC
Dimensions	29.0 inches deep x 17.1 inches wide x 3.4 inches high

System performance of QRadar Network Insights appliances varies depending on the on Inspection settings and the type and amount of network data.

For more information, see Performance impacts in the IBM QRadar Network Insights *Installation Guide*.

The following image is of the QRadar Network Insights 1940-C appliance.

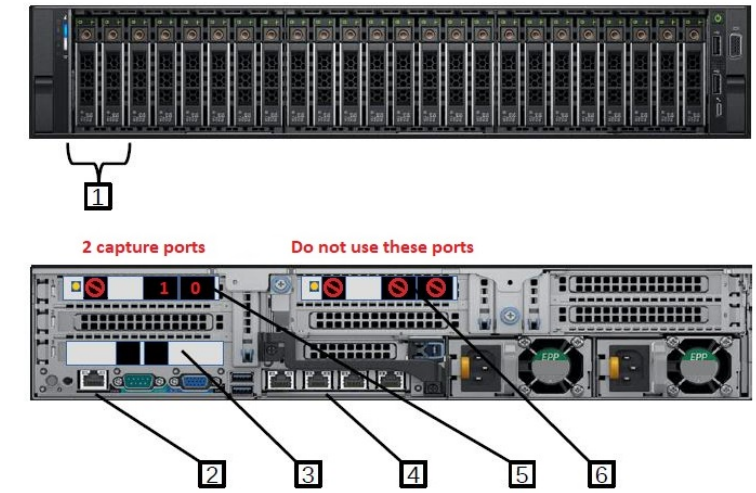


Figure 9. Front and back panel of the QRadar Network Insights 1940-C appliance

Table 19. Legend for use with the QRadar Network Insights 1940-C image	
Label	**Description**
1	QRadar system storage
2	1 x RJ-45 10/100/1000 Mb Ethernet systems management (IMM) port
3	Management ports (10 GbE SFP+)
4	Management ports (1 GbE TX)
5	Network Packet Capture (QSFP+)
6	Network Packet Capture (Unpopulated)

For information about battery replacement, see *Dell EMC PowerEdge R740 Installation and Service Manual* (https://topics-cdn.dell.com/pdf/poweredge-r740_owners-manual_en-us.pdf).

IBM QRadar Event Collector or QFlow Collector 1201/1501

The IBM QRadar QFlow Collector 1201/1501 (MTM 4563-Q5D)appliance can be used as an event collector or a QFlow collector. As a dedicated event collector, IBM QRadar QFlow Collector 1201/1501 appliance collects and parses events from various log sources and continuously forwards these events to an event processor. You can configure the IBM QRadar QFlow Collector 1201/1501 appliance to temporarily store events and only forward the stored events on a schedule. A dedicated event collector does not process events and it does not include an on-board event processor. As a QFlow collector, the appliance provides high capacity and scalable Layer 7 application data collection for distributed deployments and also supports external flow-based data sources. IBM QRadar QFlow Collector 1201/1501 is based on the Lenovo System SR630 M6.

The following table describes hardware information and requirements for the IBM QRadar QFlow Collector 1201/1501 appliance:

The following image is of the IBM QRadar QFlow Collector 1201/1501.

Table 20. IBM QRadar QFlow Collector 1201/1501 specifications	
Description	**Value**
Events per second	30,000 EPS

Table 20. IBM QRadar QFlow Collector 1201/1501 specifications (continued)	
Description	**Value**
CPU	1 x Xeon Silver 4216 16C 2.2 GHz 85W
Network management transceivers	2 x 10 GbE Short Range SFP+ The transceivers might have one of the following part numbers: • Avago AFBR-709SMZ-IB8 • Finisar FTLX8571D3BCL-BN • BNT BN-CKM-SP-SR Use these transceivers with the 2 x 10 GbE SFP+ ports, labeled as [3] in the appliance diagram
Ports	8 x 1 Gb Ethernet 2 x 10 GbE SFP+ ports 1 x RJ-45 10/100/1000 Mb Ethernet systems management (IMM) port
Memory	4 x 16 GB (64 GB)
Storage	4 x 600 GB 10K 12 Gbps SAS 2.5” / 530-8i / RAID 10
Traffic	1 Gbps
Power supply	Dual redundant 750 W AC
Dimensions	28.1 inches deep x 17.1 inches wide x 1.7 inches high

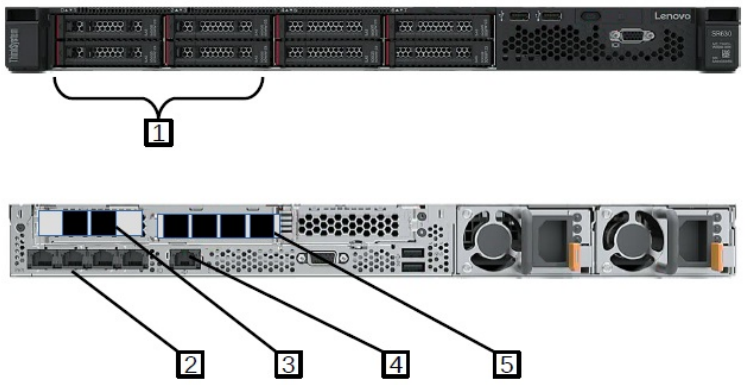


Figure 10. Front and rear panel of the IBM QRadar QFlow Collector 1201/1501

Table 21. Legend for use with the IBM QRadar QFlow Collector 1201/1501 image	
Label	**Description**
1	Event Data storage
2	Management ports (1 GbE TX)
3	10 GbE SFP+ management ports
4	1x RJ-45 10/100/1000 Mb Ethernet systems management (IMM) port
5	Event Capture ports (1 GbE TX)

For information about battery removal, see
Removing the coin-cell battery (https://thinksystem.lenovofiles.com/help/index.jsp?topic=%2F7X01%2Fcoincell_battery_replacement.html&cp=4_6_8_12).

QRadar Incident Forensics

Use the IBM QRadar Incident Forensics appliance (MTM 4563-F3A) to retrace the step-by-step actions of a potential attacker, and quickly and easily conduct an in-depth forensics investigation of suspected malicious network security incidents. QRadar Incident Forensics is based on the Lenovo System SR650 M6.

The following table describes hardware information and requirements for the QRadar Incident Forensics appliance:

Table 22. QRadar Incident Forensics specifications

Description	**Value**
CPU	2 x Xeon Silver 4214 12C 2.2 GHz 85W
Network management transceivers	2 x 10 GbE Short Range SFP+ The transceivers might have one of the following part numbers: • Avago AFBR-709SMZ-IB8 • Finisar FTLX8571D3BCL-BN • BNT BN-CKM-SP-SR Use these transceivers with the 2 x 10 GbE SFP+ ports, labeled as [4] in the appliance diagram
Ports	3 x 10/100/1000 Base-T network ports 1 x 10/100/1000 Base-T management port 1 x RJ-45 10/100/1000 Mb Ethernet systems management (IMM) port 2 x 10 GbE SFP+ ports
Memory	8 x 32 GB (256 GB)
Storage	12 x 8 TB 7.2K 12 Gbps NL SAS 930-16i 4 GB / RAID 5
Power supply	Dual redundant 750 W AC
Dimensions	28.3 inches deep x 17.5 inches wide x 3.4 inches high

The following image is of the QRadar Incident Forensics appliance.

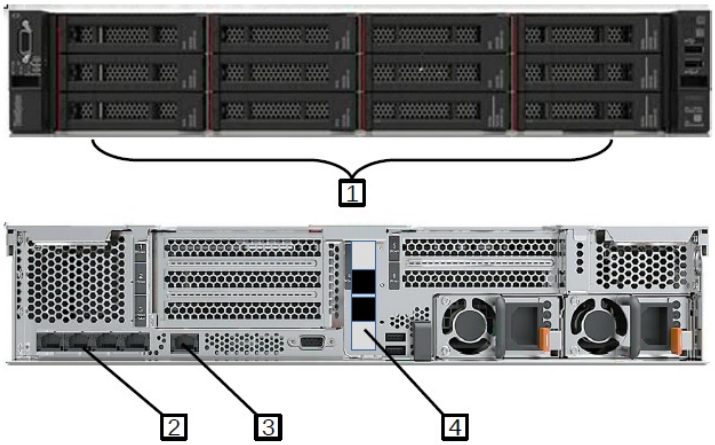


Figure 11. Front and rear panel of the QRadar Incident Forensics appliance

Table 23. Legend for use with the QRadar Incident Forensics image	
Label	**Description**
1	Event data storage
2	Management ports (1 GbE TX)
3	1x RJ-45 10/100/1000 Mb Ethernet systems management (IMM) port
4	10 Gbps SFP+ management ports

For information about battery removal, see Removing the coin-cell battery (https://thinksystem.lenovofiles.com/help/index.jsp?topic=%2F7X05%2Fcmos_battery_replacement.html&cp=4_8_8_13&anchor=CMOS_battery_replacement).

QRadar Network Packet Capture

IBM QRadar Network Packet Capture (MTM 4563-F3C) offers an optional appliance to store and manage data that is used by QRadar Incident Forensics when no other network packet capture (Network PCAP) device is deployed. Any number of these appliances can be installed as a tap on a network or subnetwork to collect the raw packet data. QRadar Network Packet Capture is based on the Lenovo System SR650 M6. Each appliance can support up to eight QRadar Network Packet Capture Direct Attached Storage (4563-D1S) units. For more information about direct attached storage, see "QRadar Network Packet Capture Direct Attached Storage" on page 34.

The following table describes hardware information and requirements for the QRadar Network Packet Capture appliance:

Table 24. QRadar Network Packet Capture specifications	
Description	**Value**
CPU	2 x Xeon Gold 6240 18C 2.6 GHz 24 MB Cache 150 W
Network capture transceivers	2 x SR 10 Gb SFP+ 2 x TX 1 Gb SFP 2 x SX 1 Gb SFP Use these transceivers with the network packet capture card, labeled as [7] in the appliance diagram.

Table 24. QRadar Network Packet Capture specifications (continued)	
Description	**Value**
Network management transceivers	2 x 10 GbE Short Range SFP+ The transceivers might have one of the following part numbers: • Avago AFBR-709SMZ-IB8 • Finisar FTLX8571D3BCL-BN • BNT BN-CKM-SP-SR Use these transceivers with the 2 x 10 GbE SFP+ ports, labeled as [5] in the appliance diagram
Ports	4 x 10/100/1000 Base-T Ethernet management ports 1 x RJ-45 10/100/1000 Mb Ethernet systems management (IMM) port 4 x Network capture ports (SFP/SFP+) (Model NT40E3-4) 2 x 10 Gbps SFP+ management ports 2 x Direct Attached Storage (DAS) ports
Memory	8 x 16 GB (128 GB)
Storage	12 x 8 TB 7.2 K 12 Gbps 3.5” NLSAS 930-16i 4 GB (RAID 5) 2 x 1 TB 7.2 K 12 Gbps 3.5” NLSAS / 930-16i 4 GB (RAID 1)
Power supply	Dual redundant 1100 W AC
Dimensions	28.3 inches deep x 17.5 inches wide (19 inches with EIA) x 3.4 inches high

The following image is of the QRadar Network Packet Capture appliance.

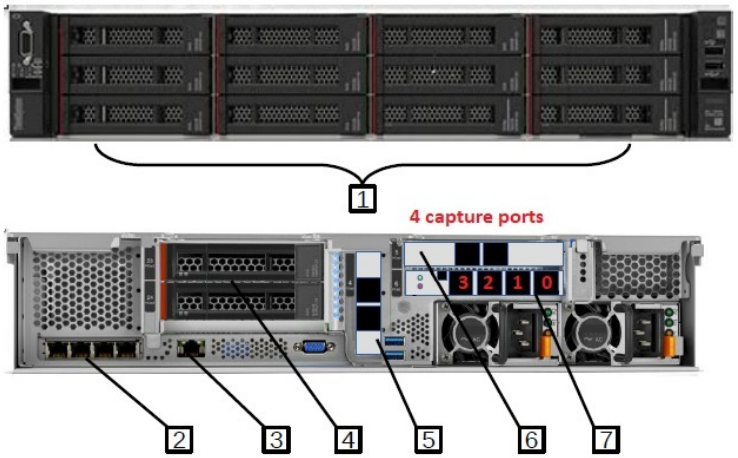


Figure 12. Front and rear panel of the QRadar Network Packet Capture appliance

Table 25. Legend for use with the QRadar Network Packet Capture image	
Label	**Description**
1	Event data storage
2	Management ports (1 GbE TX)

Table 25. Legend for use with the QRadar Network Packet Capture image (continued)	
Label	**Description**
3	1 x RJ-45 10/100/1000 Mb Ethernet systems management port
4	QRadar system storage
5	Management ports (10 GbE SFP+)
6	External DAS ports
7	Network packet capture ports (SFP/SFP+)

For information about battery removal, see Removing the coin-cell battery (https://thinksystem.lenovofiles.com/help/index.jsp?topic=%2F7X05%2Fcmos_battery_replacement.html&cp=4_8_8_13&anchor=CMOS_battery_replacement).

QRadar Network Packet Capture Direct Attached Storage

New in 7.4.1 As an option you can add the QRadar Network Packet Capture Direct Attached Storage (4563-D1S) appliance to the IBM QRadar Network Packet Capture appliance to increase the storage capacity. You can manage both the internal and external storage as a single interface. This helps reduce resource load on the system and enables easier navigation. The QRadar Network Packet Capture Direct Attached Storage appliance is based on the Lenovo D1212.

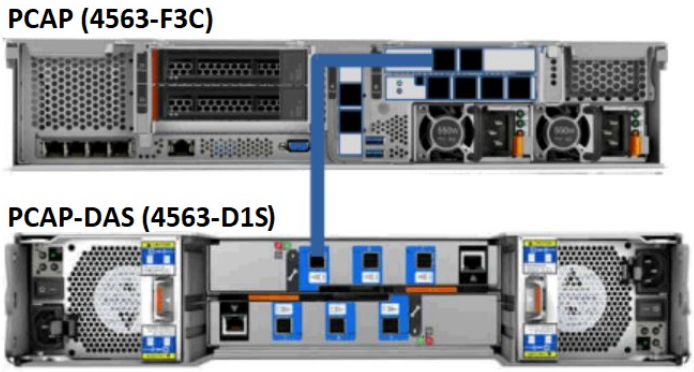
Note: You must use the Lenovo QRadar Network PCAP Direct Attached Storage appliance with the Lenovo QRadar Network Packet Capture appliance.

Table 26. QRadar Network PCAP Direct Attached Storage specifications	
Description	**Value**
Ports	3 x 12 Gb Mini-SAS 2 x 10/100 MbE management
Storage	12 x 8 TB 3.5” RAID 5 (88 TB)
Power supply	2 x 580 W AC
Dimensions	24.8 inches deep x 17.4 inches wide x 3.4 inches high

The following image is of the QRadar Network PCAP Direct Attached Storage appliance.

Figure 13. Front and rear panel of the QRadar Network PCAP Direct Attached Storage appliance

The QRadar Network Packet Capture appliance can have up to eight QRadar Network Packet Capture Direct Attached Storage (4563-D1S) storage units connected in a daisy chain configuration. The following image is of the QRadar Network Packet Capture appliance with a QRadar Network PCAP Direct Attached Storage appliance that is connected showing the wiring configuration.



The QRadar Network Packet Capture appliance can capture up to 10 Gbps. Adding QRadar Network PCAP Direct Attached Storage appliances to your Lenovo QRadar Network Packet Capture does not increase the capture rate.

QRadar Network Packet Capture-C 40 GB

New in 7.4.1 IBM QRadar Network Packet Capture-C 40 GB (MTM 4654-F3D) offers an optional appliance to store and manage data that is used by QRadar Incident Forensics. Any number of these appliances can be installed as a tap on a network or subnetwork to collect the raw packet data. QRadar Network Packet Capture-C 40 GB is based on the Dell R740xd XL server. Each appliance can support up to three QRadar Network Packet Capture-C Direct Attached Storage (4654-D2S) units. For more information about direct attached storage, see “QRadar Network Packet Capture-C Direct Attached Storage” on page 37.

The following table describes hardware information and requirements for the QRadar Network Packet Capture-C 40 GB appliance:

Table 27. QRadar Network Packet Capture-C 40 GB specifications	
Description	**Value**
CPU	2 x Xeon Gold 6240 20C 2.6 GHz 24 MB Cache 150 W
Network capture transceivers	2 x 40 GbE SR4 QSFP+ transceivers (Finisar FTL410QD2C) Use these transceivers with the network packet capture card, labeled as [3] in the appliance diagram.
Network management transceivers	2 x 10 GbE Short Range SFP+ The transceivers might have one of the following part numbers: • Avago AFBR-709SMZ-IB8 • Finisar FTLX8571D3BCL-BN • BNT BN-CKM-SP-SR Use these transceivers with the 2 x 10 GbE SFP+ management ports, labeled as [6] in the appliance diagram.
Ports	4 x 10/100/1000 Base-T Ethernet management ports 1 x RJ-45 10/100/1000 Mb Ethernet systems management (IMM) port 2 x 40 GbE SR4 QSFP+ ports (Model NT200A02) 2 x 10 Gbps SFP+ management ports 3 x Direct Attached Storage (DAS) ports
Memory	8 x 16 GB (128 GB)
Storage	12 x 8 TB 7.2 K 12 Gbps 3.5” NLSAS / PERC H740P RAID 5 2 x 1.2 TB 10 K 12 ps 2.5” SAS / PERC H740 GbP RAID 1
Power supply	Dual redundant 1100 W AC
Dimensions	29.0 inches deep x 17.1 inches wide x 3.4 inches high

The following image is of the QRadar Network Packet Capture-C 40 GB appliance.

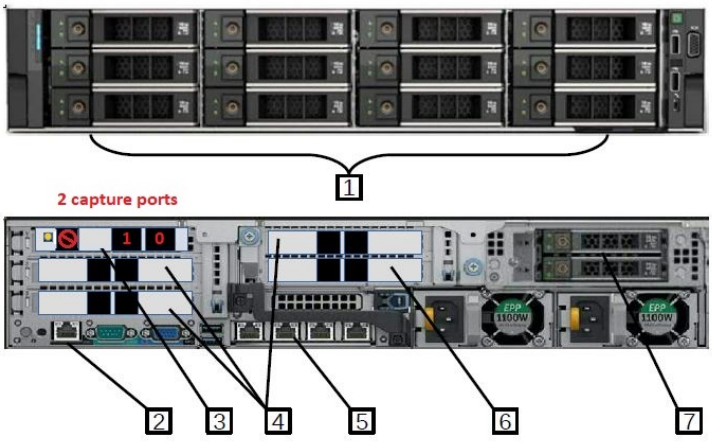


Figure 14. Front and rear panel of the QRadar Network Packet Capture-C 40 GB appliance

Table 28. Legend for use with the QRadar Network Packet Capture-C 40 GB image	
Label	**Description**
1	Event data storage
2	1x RJ-45 10/100/1000 Mb Ethernet systems management (IMM) port
3	2 x 40 GbE SR4 QSFP+ network capture ports
4	External RAID DAS ports
5	Management ports (1 GbE TX)
6	Management ports (10 GbE SFP+)
7	QRadar firmware storage

For information about battery replacement, see *Dell EMC PowerEdge R740 Installation and Service Manual* (https://topics-cdn.dell.com/pdf/poweredge-r740_owners-manual_en-us.pdf).

QRadar Network Packet Capture-C Direct Attached Storage

New in 7.4.1 As an option you can add the QRadar Network Packet Capture Direct Attached Storage appliance to the QRadar Network Packet Capture-C 40 GB appliance to increase the storage capacity. You can manage both the internal and external storage as a single interface. This helps reduce resource load on the system and enables easier navigation. The QRadar Network PCAP-C Direct Attached Storage appliance is based on the Dell MD1400.

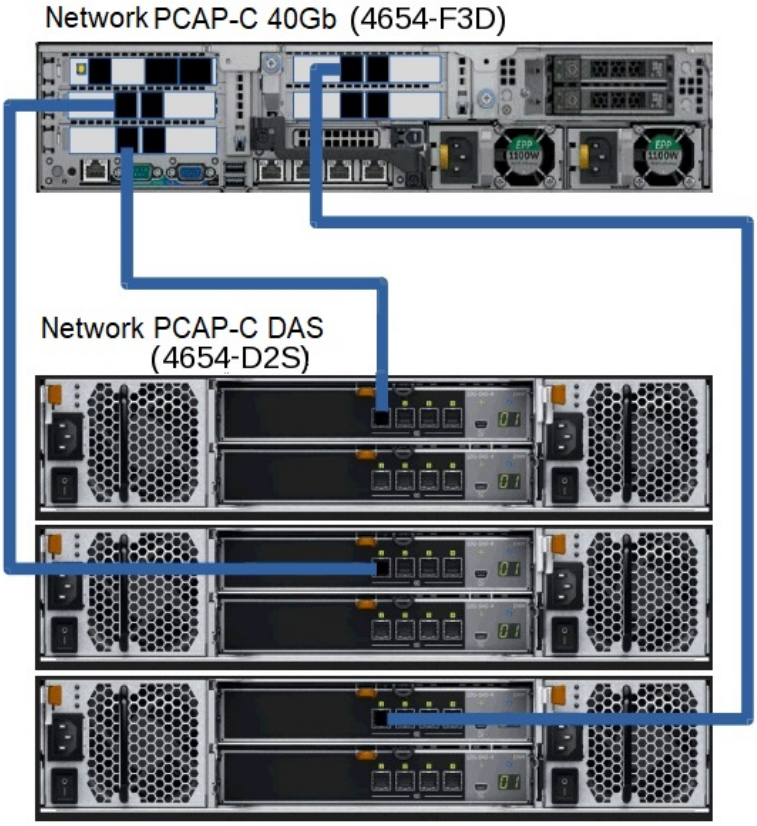
Note: You must use the Dell QRadar Network PCAP-C Direct Attached Storage appliance with the Dell QRadar Network Packet Capture-C 40 GB appliance.

Table 29. QRadar Network PCAP-C Direct Attached Storage specifications	
Description	**Value**
Ports	4x 12 Gb Mini-SAS
Storage	12 x 8 TB 3.5” RAID 5 (88 TB)
Power supply	AC - 600 W
Dimensions	23.3 inches deep x 18.9 inches wide x 3.4 inches high

The following image is of the QRadar Network PCAP-C Direct Attached Storage appliance.

Figure 15. Front and rear panel of the QRadar Network PCAP-C Direct Attached Storage appliance

The QRadar Network Packet Capture-C 40 GB can have up to three QRadar Network PCAP-C Direct Attached Storage storage units connected. The following image is of the QRadar Network Packet Capture-C 40 GB appliance with three QRadar Network PCAP-C Direct Attached Storage appliances that are connected showing the wiring configuration.



Without a DAS unit, the QRadar Network Packet Capture-C 40 GB appliance can capture up to 10 Gbps. Each additional QRadar Network PCAP-C Direct Attached Storage appliance that is connected increases the capture rate by 10 Gbps.

Chapter 3. QRadar M5 appliance overview

Review information about IBM QRadar to understand hardware and license requirements.

Review this overview of QRadar appliances, including capabilities, and license limitations.

IBM QRadar appliances are certified to support a certain maximum events per second (EPS) rate. Maximum EPS depends on the type of data that is processed, system configuration, and system load. For more information, see QRadar maximum EPS certification methodology.

Integrated Management Module

The Integrated Management Module (IMM) is a management module that is used for systems-management functions.

On the back panel of each appliance type, the serial connector and Ethernet connectors can be managed by using the Integrated Management Module (IMM). You can configure the IMM to share an Ethernet port with the IBM QRadar management interface; however, you can configure the IMM in dedicated mode to reduce the risk of losing the IMM connection when the appliance is restarted. To configure the IMM, you must access the System BIOS settings by pressing the F1 key when the IBM splash screen is displayed. For further instructions on how to configure the IMM, see the *Integrated Management Module User's Guide* that comes with your appliance.

QRadar xx05

Use the IBM QRadar xx05 (MTM 4412-Q1E) appliance for various appliance types in your deployment.

Use the QRadar xx05 for the following appliance types:

- QRadar Event Processor 1605
- QRadar Flow Processor 1705
- QRadar 1805 Event and Flow Processor
- QRadar 3105 (All-in-One)
- QRadar 3105 (Console)
- QRadar Log Manager 1605
- QRadar Log Manager 3105 (All-in-One)
- QRadar Log Manager 3105 Console
- QRadar Risk Manager
- QRadar Vulnerability Manager
- QRadar App Host
- QRadar 1400 Data Node

View hardware information and requirements for the QRadar xx05 in the following table:

Table 30. QRadar xx05 overview

Description	Value
Maximum capacity	QRadar Event Processor 1605: 20,000 EPS QRadar Flow Processor 1705: 1,200,000 FPM QRadar 1805 Event and Flow Processor: 5000 EPS, 200,000 FPM QRadar 3105 (All-in-One): 5000 EPS, 200,000 FPM

Table 30. QRadar xx05 overview (continued)	
Description	**Value**
CPU	2 x E5-2620 V4 2.1GHz 8C 20MB 2133MHz 85W
Network management transceivers	2 x 10 GbE Short Range SFP+ The transceivers might have one of the following part numbers: • Avago AFBR-709SMZ-IB8 • Finisar FTLX8571D3BCL-BN • BNT BN-CKM-SP-SR Use these transceivers with the 2 x 10 GbE SFP+ ports, labeled as [5] in the appliance diagram
Ports	2 x 8 Gbps Fibre Channel HBA ports 4 x 10/100/1000 Base T Ethernet ports 1 x RJ-45 10/100/1000 Mb Ethernet systems management (IMM) port 2 x 10 GbE SFP+ Ethernet ports
Memory	64 GB 2400 MHz DDR4 RDIMM
Storage	10 x 2.5 inch 1 TB 7.2 K rpm NL SAS, 8 TB total (RAID 6), 5.6 TB available to store event and flow data
Power supply	Dual redundant 750W AC power supply
Dimensions	28.9 inches deep x 17.1 inches wide x 1.7 inches high
Included components	Event Collector Event Processor for processing events Internal storage for events QRadar Data Node appliance

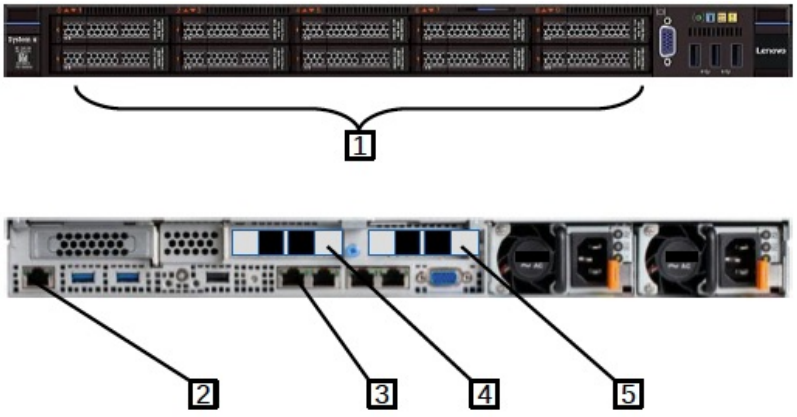


Figure 16. QRadar xx05

Table 31. Legend for use with the QRadar xx05 image	
Label	**Description**
1	Event data storage

Table 31. Legend for use with the QRadar xx05 image (continued)	
Label	**Description**
2	1 x RJ-45 10/100/1000 Mb Ethernet systems management (IMM) port
3	Management ports (1 GbE TX)
4	Fibre channel ports (8 Gb SFP+)
5	Management ports (10 GbE SFP+)

You can upgrade your license to migrate your QRadar Log Manager 3105 (All-in-One) to QRadar 3105 (All-in-One). For more information, see *QRadar Log Manager to QRadar SIEM Migration Guide*.

For battery removal steps, see Removing the coin-cell battery (http://publib.boulder.ibm.com/infocenter/systemx/documentation/index.jsp?topic=/com.lenovo.sysx.8871.doc/t_removing_system_battery.html).

"QRadar xx05" on page 39 is based on the Lenovo System x3550 M5.

For more information about the front panel, see Front view (http://publib.boulder.ibm.com/infocenter/systemx/documentation/index.jsp?topic=/com.lenovo.sysx.8869.doc/c_front_view.html).

For more information about the back panel, see Rear view (http://publib.boulder.ibm.com/infocenter/systemx/documentation/index.jsp?topic=/com.lenovo.sysx.8869.doc/c_rear_view.html).

QRadar xx29

Use the IBM QRadar xx29 (MTM 4412-Q2A) for various appliance types in your deployment.

The QRadar xx29 can be used for the following appliances:

- QRadar Event Processor 1629
- QRadar Flow Processor 1729
- QRadar Event and Flow Processor 1829
- QRadar 3129 (All-in-One)
- QRadar 3129 (Console)
- QRadar Log Manager 1629
- QRadar Log Manager 3129 (All-in-One)
- QRadar Log Manager 3129 (Console)
- QRadar App Host
- QRadar 1400 Data Node

View hardware information and requirements for the QRadar xx29 in the following table:

Table 32. QRadar xx29	
Description	**Value**
Maximum capacity	QRadar Event Processor 1629: 40,000 EPS QRadar Flow Processor 1729: 2,400®,000 FPM QRadar Event and Flow Processor 1829: : 15,000 EPS, 300,000 FPM QRadar 3129 (All-in-One): 15,000 EPS, 300,000 FPM
CPU	2 x E5-2650 v4 12C 2.2 GHz 30 MB 2400 MHz 105W

Table 32. QRadar xx29 (continued)	
Description	**Value**
Network management transceivers	2 x 10 GbE Short Range SFP+ The transceivers might have one of the following part numbers: • Avago AFBR-709SMZ-IB8 • Finisar FTLX8571D3BCL-BN • BNT BN-CKM-SP-SR Use these transceivers with the 2 x 10 GbE SFP+ ports, labeled as [3] in the appliance diagram.
Ports	2 x 8 Gbps Fibre Channel HBA ports 4 x 10/100/1000 Base-T Ethernet ports 1 x RJ-45 10/100/1000 Mb Ethernet systems management (IMM) port 2 x 10 GbE SFP+ ports
Memory	128 GB, 8 x 16 GB 2400 MHz DDR4 RDIMM
Storage	12 x 3.5 inches 6 TB SAS 7.2 K rpm, 60 TB total (RAID6) 3129: 48 TB available to store event and flow data. All other xx29 appliances: 58 TB available to store event and flow data.
Power supply	Dual Redundant 900 W AC
Dimensions	29.7 inches deep x 17.1 inches wide x 3.4 inches high
Included components	Event Collector Event Processor for processing events and flows Internal storage for events and flows QRadar Data Node appliance

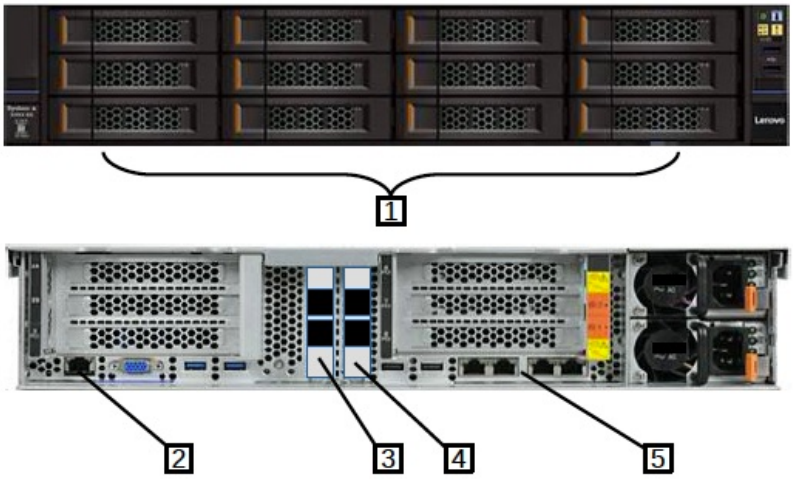


Figure 17. QRadar xx29

Table 33. Legend for use with the QRadar xx29 image	
Label	**Description**
1	Event data storage
2	1 x RJ-45 10/100/1000 Mb Ethernet systems management (IMM) port
3	Management ports (10 GbE SFP+)
4	Fibre channel ports (8 Gb SFP+)
5	Management ports (1 GbE TX)

For battery removal steps, see Removing the coin-cell battery (also called CMOS battery) (http://publib.boulder.ibm.com/infocenter/systemx/documentation/index.jsp?topic=/com.lenovo.sysx.8871.doc/t_removing_system_battery.html).

For more information about the front panel, see Front view (http://publib.boulder.ibm.com/infocenter/systemx/documentation/index.jsp?topic=/com.lenovo.sysx.8871.doc/c_front_view.html).

For more information about the back panel, see Rear view (http://publib.boulder.ibm.com/infocenter/systemx/documentation/index.jsp?topic=/com.lenovo.sysx.8871.doc/c_rear_view.html).

For more information, you can also see System x3650 M5 (https://lenovopress.com/lp0068-lenovo-system-x3650-m5-machine-type-8871.html).

QRadar xx29-C

The IBM QRadar xx29-C (MTM 4654-Q3A) supports various appliance types in your deployment.

The QRadar xx29-C appliance can be used for the following appliance types:

- QRadar Event Processor 1629
- QRadar Flow Processor 1729
- QRadar Event and Flow Processor 1829
- QRadar 3129 (All-in-One)
- QRadar 3129 (Console)
- QRadar Log Manager 1629
- QRadar Log Manager 3129 (All-in-One)
- QRadar Log Manager 3129 (Console)
- QRadar App Host
- QRadar 1400 Data Node

View hardware information and requirements for the QRadar xx29-C in the following table:

The following table describes hardware information and requirements for the QRadar xx29-C appliance:

Table 34. QRadar xx29-C specifications	
Description	**Value**
Maximum capacity	QRadar Event Processor 1629: 40,000 EPS QRadar Flow Processor 1729: 2,400,000 FPM QRadar Event and Flow Processor 1829: : 15,000 EPS, 300,000 FPM QRadar 3129 (All-in-One): 15,000 EPS, 300,000 FPM
CPU	2 x Xeon Gold 5118 12C 2.3 GHz 16 MB Cache 3.20 GHz 105 W

Table 34. QRadar xx29-C specifications (continued)	
Description	**Value**
Network management transceivers	2 x 10 GbE Short Range SFP+ The transceivers might have one of the following part numbers: • Avago AFBR-709SMZ-IB8 • Finisar FTLX8571D3BCL-BN • BNT BN-CKM-SP-SR Use these transceivers with the 2 x 10 GbE SFP+ ports, labeled as [3] in the appliance diagram.
Ports	2 x 16 Gbps Fibre Channel HBA ports 4 x 10/100/1000 Base-T Ethernet management ports 1 x RJ-45 10/100/1000 Mb Ethernet systems management (IMM) port 2 x 10 GbE SFP+ Ethernet management ports
Memory	128 GB, 8 x 16 GB 1866 MHz RDIMM
Storage	12 x 8 TB 7.2 K 12 Gbps 512e 3.5” NLSAS, 80 TB total (RAID6) 68 TB available to store event and flow data.
Power supply	Dual redundant 1100 W AC
Unit weight	73 lbs
Physical dimensions	29.0 inches deep x 17.1 inches wide x 3.4 inches high

The following image is of the QRadar xx29-C appliance.

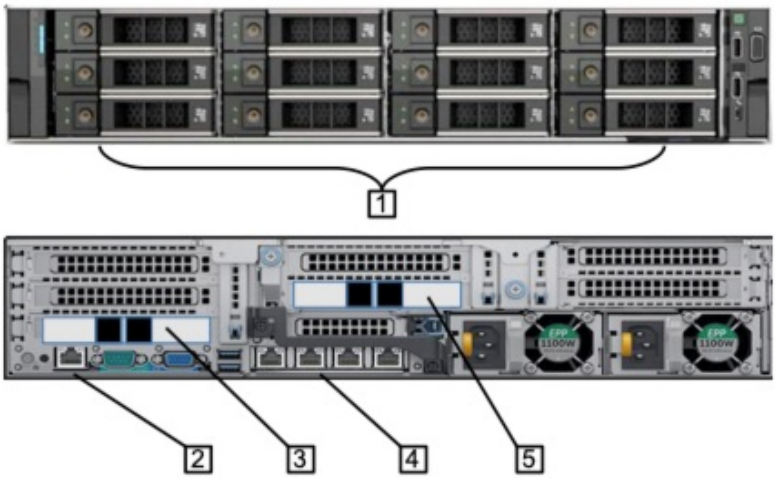


Figure 18. Front and rear panel of the QRadar xx29-C appliance

Table 35. Legend for use with the QRadar xx29-C image	
Label	**Description**
1	Event data storage
2	1 x RJ-45 10/100/1000 Mb Ethernet systems management (IMM) port

Table 35. Legend for use with the QRadar xx29-C image (continued)	
Label	**Description**
3	Management ports (10 GbE SFP+)
4	Management ports (1 GbE TX)
5	Fibre channel ports (16 Gb SFP+)

For information about battery replacement, see *Dell EMC PowerEdge R740 Installation and Service Manual* (https://topics-cdn.dell.com/pdf/poweredge-r740_owners-manual_en-us.pdf).

QRadar xx48

The IBM QRadar xx48 (MTM 4412-Q3B) captures logs from sources that generate a large amount of traffic without a need for load balancing.

The QRadar xx48 appliance handles the higher levels of performance that are required by enterprise class clients. For example, companies can use the QRadar xx48 for the following requirements:

- A company wants faster processing to search and analyze a large amount of data.
- A company wants to reduce the footprint of an IBM QRadar deployment, so they install QRadar xx48 appliances to reduce rack space.

The following appliances are examples of appliance types that you can use the QRadar xx48 for:

- QRadar Event Processor 1648
- QRadar Flow Processor 1748
- QRadar Event and Flow Processor 1848
- QRadar 3148 (All-in-One)
- QRadar 3148 (Console)
- QRadar App Host
- QRadar 1400 Data Node

View hardware information and requirements for the QRadar xx48 in the following table:

Table 36. QRadar xx48 overview	
Description	**Value**
Maximum capacity	QRadar Event Processor 1648: 80,000 EPS QRadar Flow Processor 1748: 3,600,000 FPM QRadar Event and Flow Processor 1848: 30,000 EPS, 1,200,000 FPM QRadar 3148 (All-in-One): 30,000 EPS, 1,200,000 FPM
CPU	2 x E5-2680 v4 14C 2.4 GHz 35 MB 2400 MHz 120W
Network management transceivers	2 x 10 GbE Short Range SFP+ The transceivers might have one of the following part numbers: • Avago AFBR-709SMZ-IB8 • Finisar FTLX8571D3BCL-BN • BNT BN-CKM-SP-SR Use these transceivers with the 2 x 10 GbE SFP+ ports, labeled as [3] in the appliance diagram.

Table 36. QRadar xx48 overview (continued)	
Description	**Value**
Ports	2 x 8 Gbps Fibre Channel HBA ports 4 x 10/100/1000 Base-T Ethernet ports 1 x RJ-45 10/100/1000 Mb Ethernet systems management (IMM) port 2 x 10 Gbps SFP+ ports
Memory	128 GB, 2133 MHz DDR4 RDIMM
Storage	6x 3.8 TB SSD
Power supply	Dual redundant 900 W AC
Dimensions	31.5 inches deep x 17.5 inches wide (19 inches with EIA) x 3.4 inches high

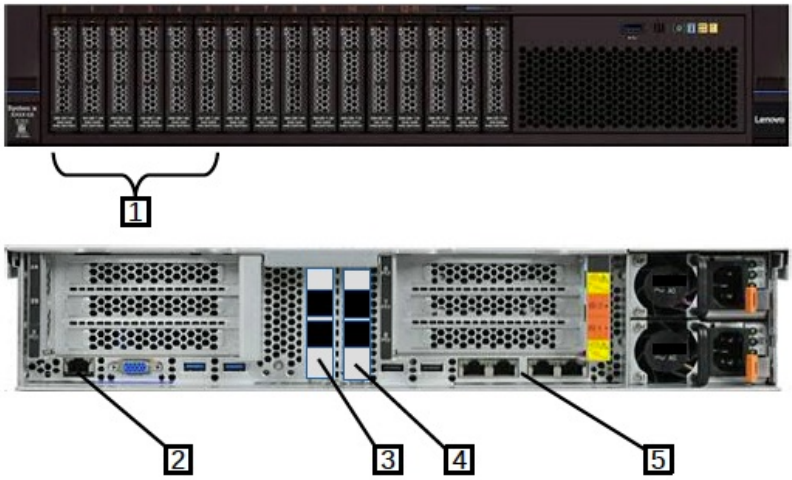


Figure 19. QRadar xx48

Table 37. Legend for use with the QRadar xx48 image	
Label	**Description**
1	Event data storage
2	1 x RJ-45 10/100/1000 Mb Ethernet systems management (IMM) port
3	Management ports (10 GbE SFP+)
4	Fibre channel ports (8 Gb SFP+)
5	Management ports (1 GbE TX)

For battery removal steps, see Removing the coin-cell battery (also called CMOS battery) (http://www-01.ibm.com/support/knowledgecenter/api/redirect/systemx/documentation/index.jsp?topic=/com.lenovo.sysx.8871.doc/t_removing_system_battery.html).

For more information about the front panel, see Front view (http://www-01.ibm.com/support/knowledgecenter/api/redirect/systemx/documentation/index.jsp?topic=/com.lenovo.sysx.8871.doc/c_front_view.html).

For more information about the back panel, see Rear view (http://www-01.ibm.com/support/knowledgecenter/api/redirect/systemx/documentation/index.jsp?topic=/com.lenovo.sysx.8871.doc/c_rear_view.html).

For more information, you can also see System x3650 M5 (https://lenovopress.com/lp0068-lenovo-system-x3650-m5-machine-type-8871.html).

QRadar xx48-C

The IBM QRadar xx48-C (MTM 4654-Q4B) captures logs from sources that generate a large amount of traffic without a need for load balancing.

The QRadar xx48-C appliance handles the higher levels of performance that are required by enterprise class clients. For example, companies can use the QRadar xx48-C for the following requirements:

- A company wants faster processing to search and analyze a large amount of data.
- A company wants to reduce the footprint of an IBM QRadar deployment, so they install QRadar xx48-C appliances to reduce rack space.

The following appliances are examples of appliance types that you can use the QRadar xx48-C for:

- QRadar Event Processor 1648
- QRadar Flow Processor 1748
- QRadar Event and Flow Processor 1848
- QRadar 3148 (All-in-One)
- QRadar 3148 (Console)
- QRadar App Host
- QRadar 1400 Data Node

View hardware information and requirements for the QRadar xx48-C in the following table.

Table 38. QRadar xx48-C overview

Description	**Value**
Maximum capacity	QRadar Event Processor 1648: 80,000 EPS QRadar Flow Processor 1748: 3,600,000 FPM QRadar Event and Flow Processor 1848: 30,000 EPS, 1,200,000 FPM QRadar 3148 (All-in-One): 30,000 EPS, 1,200,000 FPM
CPU	2 x Xeon Gold 6132 14C 2.6 GHz 19 MB Cache 3.70 GHz 140 W
Network management transceivers	2 x 10 GbE Short Range SFP+ The transceivers might have one of the following part numbers: • Avago AFBR-709SMZ-IB8 • Finisar FTLX8571D3BCL-BN • BNT BN-CKM-SP-SR Use these transceivers with the 2 x 10 GbE SFP+ ports, labeled as [3] in the appliance diagram
Ports	2 x 16 Gbps Fibre Channel HBA ports 4 x 10/100/1000 Base-T Ethernet ports 1 x RJ-45 10/100/1000 Mb Ethernet systems management (IMM) port 2 x 10 Gbps SFP+ ports
Memory	128 GB, 8 x 16 GB 1866 MHz RDIMM

Table 38. QRadar xx48-C overview (continued)	
Description	**Value**
Storage / Hard disks	6 x 3.84 TB 12 Gb SAS 2.5" SSD, 15.36 TB Total (RAID6) 12 TB available to store event and flow data.
Power supply	Dual redundant 1100 W AC
Unit weight	48.5 lbs
Physical dimensions	31.3 inches deep x 17.1 inches wide x 1.7 inches high

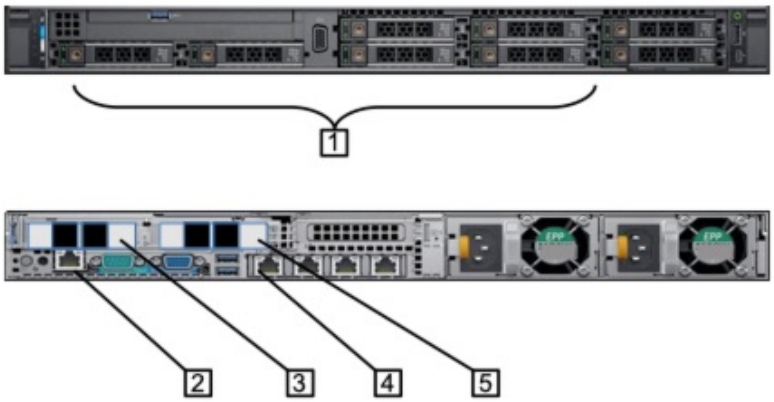


Figure 20. QRadar xx48-C

Table 39. Legend for use with the QRadar xx48-C image	
Label	**Description**
1	Event data storage
2	1 x RJ-45 10/100/1000 Mb Ethernet systems management (IMM) port
3	Management ports (10 GbE SFP+)
4	Management ports (1 GbE TX)
5	Fibre channel ports (16 Gb SFP+)

For information about battery replacement, see *Dell EMC PowerEdge R640 Installation and Service Manual* (https://topics-cdn.dell.com/pdf/poweredge-r640_owners-manual_en-us.pdf).

QRadar QFlow Collector 1202/1301

The IBM QRadar QFlow Collector 1202/1301 (MTM 4412-Q7C) appliance provides high capacity and scalable Layer 7 application data collection for distributed deployments. The QRadar QFlow Collector 1202/1301 also supports external flow-based data sources.

This appliance is only available by special order.

View the hardware information and requirements for the QRadar QFlow Collector 1202/1301 in the following table.

Table 40. QRadar QFlow Collector 1202/1301 overview	
Description	**Value**
CPU	1 x E5-2680 v4 14C 2.4 GHz 35 MB Cache 2400 MHz 120W

Table 40. QRadar QFlow Collector 1202/1301 overview (continued)	
Description	**Value**
Memory	64 GB, 4 x 16 GB truDDR4 2133 MHz Memory
Storage	2 x 240 GB SATA 2.5" SSD, 240 GB Total (RAID1)
Network capture transceivers	4 x 1 G TX RJ-45 Transceivers (Avago ABCU-5710RZ or ABCU-5740RZ) 4 x 1 G SX LC Transceivers (Avago AFBR-5715PZ) Use these transceivers with the network packet capture card, labeled as [4] in the appliance diagram.
Network management transceivers	2 x 10 GbE Short Range SFP+ The transceivers can have one of the following part numbers: • Avago AFBR-709SMZ-IB8 • Finisar FTLX8571D3BCL-BN • BNT BN-CKM-SP-SR Use these transceivers with the 2 x 10 GbE SFP+ ports, labeled as [5] in the appliance diagram.
Ports	4 x 1 Gb Ethernet ports 1 x RJ-45 10/100/1000 Mb Ethernet systems management (IMM) port Network Packet Capture (SFP/SFP+) ports 2 x 10 Gbps SFP+ management ports
Traffic	3 Gbps
Power supply	Dual redundant 750 W AC
Dimensions	28.9 inches deep x 17.1 inches wide x 1.7 inches high

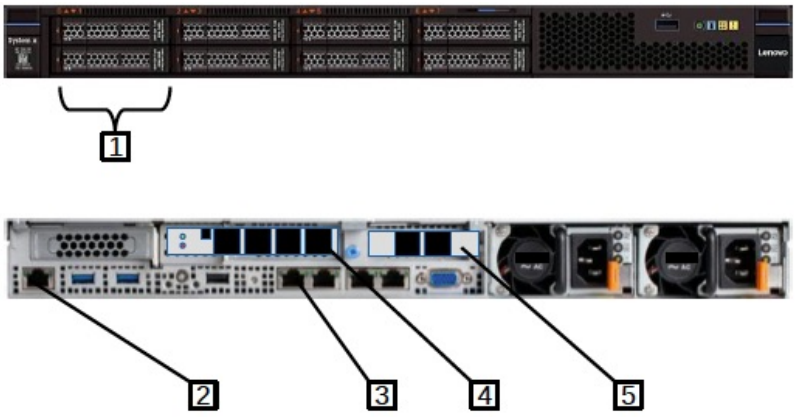


Figure 21. QRadar QFlow Collector 1202/1301

Table 41. Legend for use with the QRadar QFlow Collector 1202/1301 image	
Label	**Description**
1	QRadar firmware storage
2	IMM port (1 GbE TX)

Table 41. Legend for use with the QRadar QFlow Collector 1202/1301 image (continued)	
Label	**Description**
3	Management ports (1 GbE TX)
4	Network packet capture (SFP)
5	Management ports (10 GbE SFP+)

For battery removal steps, see Removing the coin-cell battery (also called CMOS battery) (http://www-01.ibm.com/support/knowledgecenter/api/redirect/systemx/documentation/index.jsp?topic=/com.lenovo.sysx.8871.doc/t_removing_system_battery.html)

For more information about the QRadar QFlow Collector 1202/1301 including front and back panel diagrams, see IBM System X3550 M5 (https://lenovopress.com/lp0067-lenovo-system-x3550-m5-machine-type-8869).

QRadar QFlow Collector 1310

The IBM QRadar QFlow Collector 1310 (MTM 4412-Q8C) appliance provides high capacity and scalable Layer 7 application data collection for distributed deployments. The QRadar QFlow Collector 1310 also supports external flow-based data sources.

This appliance is only available by special order.

View hardware information and requirements for the QRadar QFlow Collector 1310 in the following table.

Table 42. QRadar QFlow Collector 1310 overview	
Description	**Value**
CPU	1 x E5-2680 v4 14C 2.4 GHz 35 MB Cache 2400 MHz 120W
Memory	64 GB, 4 x16 GB truDDR4 2133 MHz Memory
Storage	2 x 240 GB SATA 2.5" SSD, 240 GB Total (RAID1)
Network capture transceivers	4 x 1 G TX RJ-45 Transceivers (Avago ABCU-5710RZ or ABCU-5740RZ) 4 x 1 G SX LC Transceivers (Avago AFBR-5715PZ) Use these transceivers with the network packet capture card, labeled as [4] in the appliance diagram.
Network management transceivers	2 x 10 GbE Short Range SFP+ The transceivers can have one of the following part numbers: • Avago AFBR-709SMZ-IB8 • Finisar FTLX8571D3BCL-BN • BNT BN-CKM-SP-SR Use these transceivers with the 2 x 10 GbE SFP+ ports, labeled as [5] in the appliance diagram.
Ports	4 x 1 Gb Ethernet ports 1 x RJ-45 10/100/1000 Mb Ethernet systems management (IMM) port Network Packet Capture (SFP/SFP+) ports 2 x 10 Gbps SFP+ ports
Network traffic	10 Gbps

Table 42. QRadar QFlow Collector 1310 overview (continued)	
Description	**Value**
Power supply	Dual redundant 750 W AC
Dimensions	28.9 inches deep x 17.1 inches wide x 1.7 inches high

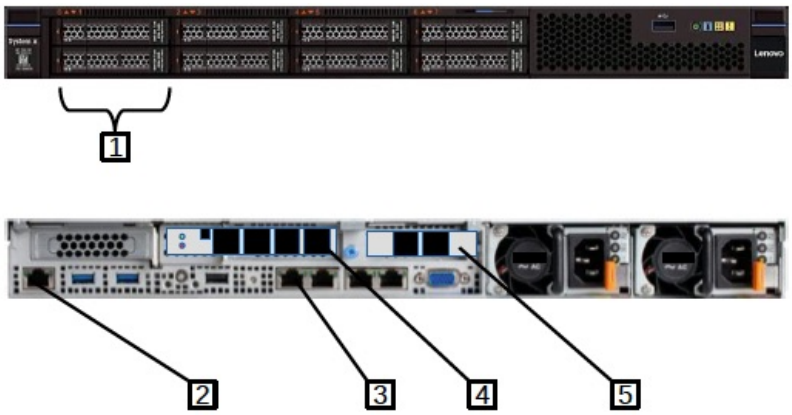


Figure 22. QRadar QFlow Collector 1310

Table 43. Legend for use with the QRadar QFlow Collector 1310 image	
Label	**Description**
1	QRadar Firmware Storage
2	IMM port (1 GbE TX)
3	Management ports (1 GbE TX)
4	Network Packet Capture (SFP/SFP+)
5	Management ports (10 GbE SFP+)

For battery removal steps, see Removing the coin-cell battery (also called CMOS battery) (http://www-01.ibm.com/support/knowledgecenter/api/redirect/systemx/documentation/index.jsp?topic=/com.lenovo.sysx.8871.doc/t_removing_system_battery.html)

For more information about the QRadar QFlow Collector 1310 including front and back panel diagrams, see IBM System X3550 M5 (https://lenovopress.com/lp0067-lenovo-system-x3550-m5-machine-type-8869).

QRadar Event Collector 1501

The IBM QRadar Event Collector 1501 (MTM 4412-Q4D) appliance is a dedicated event collector. By default, a dedicated event collector collects and parses event from various log sources and continuously forwards these events to an event processor. You can configure the QRadar Event Collector 1501 appliance to temporarily store events and only forward the stored events on a schedule. A dedicated event collector does not process events and it does not include an on-board event processor.

Tip: You can configure the QRadar Event Collector 1501 appliance to be used as a QRadar QFlow Collector 1201.

View hardware information and requirements for the QRadar Event Collector 1501 in the following table:

Table 44. QRadar Event Collector 1501 specifications	
Description	**Value**
Events per second	**15,000 EPS**
CPU	1 x E5-2620 v4 8C 2.1 GHz 20 MB Cache 2133 MHz
Network management transceivers	2 x 10 GbE Short Range SFP+ The transceivers might have one of the following part numbers: • Avago AFBR-709SMZ-IB8 • Finisar FTLX8571D3BCL-BN • BNT BN-CKM-SP-SR Use these transceivers with the 2 x 10 GbE SFP+ ports, labeled as [5] in the appliance diagram.
Ports	1 x RJ-45 10/100/1000 Mb Ethernet systems management (IMM) port 8 x 10/100/1000 Base-T Ethernet ports 2 x 10 GbE SFP+ ports
Memory	64 GB, 4 x 16 GB truDDR4 2400 MHz LP RDIMM
Storage	4 x 600 GB 2.5 inches 10 K rpm 12 Gbps SAS RAID 10 1.2 GB total (RAID 10)
Traffic	1 Gbps
Power supply	System x 550 W High Efficiency Platinum AC Power Supply
Dimensions	28.9 inches deep x 17.1 inches wide x 1.7 inches high
Included components	Event Collector

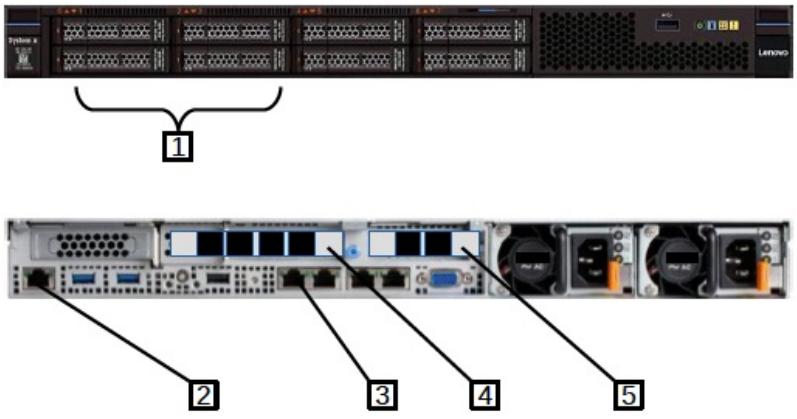


Figure 23. QRadar Event Collector 1501

Table 45. Legend for use with the QRadar Event Collector 1501 image	
Label	**Description**
1	Event data storage
2	1 x RJ-45 10/100/1000 Mb Ethernet systems management (IMM) port
3	Management ports (1 GbE TX)

Table 45. Legend for use with the QRadar Event Collector 1501 image (continued)	
Label	**Description**
4	Event capture ports (1 GbE TX)
5	10 GbE SFP+ management ports

For more information about the QRadar Event Collector 1501 including front and back panel diagrams, see IBM System X3550 M5 (https://lenovopress.com/lp0067-lenovo-system-x3550-m5-machine-type-8869).

QRadar Network Insights 1901

The IBM QRadar Network Insights 1901 (MTM 4412-F4Y) appliance provides detailed analysis of network flows to extend the threat detection capabilities of IBM QRadar.

With four 1G capture ports on a Napatech card, the QRadar Network Insights 1901 appliance provides the same capabilities as the QRadar Network Insights 1920 appliance but on a lower-price hardware platform that is designed for 1 Gbps network connectivity.

The QRadar Network Insights 1901 appliance has the following hardware specifications:

Table 46. QRadar Network Insights 1901 overview	
Hardware	**Description**
CPU	1 x E5-2680 v4 2.4 GHz 14C 2.4 GHz 35 MB Cache 2400 MHz 120W
Network capture transceivers	4 x 1 G TX RJ-45 Transceivers (Avago ABCU-5710RZ or ABCU-5740RZ) 4 x 1 G SX LC Transceivers (Avago AFBR-5715PZ) Use these transceivers with the network packet capture card, labeled as [4] in the appliance diagram.
Network management transceivers	2 x 10 GbE Short Range SFP+ The transceivers might have one of the following part numbers: • Avago AFBR-709SMZ-IB8 • Finisar FTLX8571D3BCL-BN • BNT BN-CKM-SP-SR Use these transceivers with the 2 x 10 GbE SFP+ ports, labeled as [5] in the appliance diagram.
Ports	4 x 1 Gb Ethernet ports 2 x 10 GbE SFP+ ports 1 x RJ-45 10/100/1000 Mb Ethernet systems management (IMM) port 4 x Network capture ports (SFP)
Storage	2 x 240 GB SATA 2.5" SSD, 480 GB Total (RAID1) OR 2 x 200 GB SATA 2.5" SSD, 400 GB Total (RAID1) The storage is labeled as [1] in the appliance diagram.
Memory	64 GB (4 x 16 GB DDR4 2400 MHz)

Table 46. QRadar Network Insights 1901 overview (continued)	
Hardware	**Description**
Traffic	1 Gbps
Power	Dual redundant 750-Watt AC power supply
Dimensions	28.9 inches deep x 17.1 inches wide x 1.7 inches high

System performance of QRadar Network Insights appliances varies depending on the exact configuration and tuning of the system components. It is influenced not only by hardware, but also factors such as the search, extraction criteria, and the amount of network data. For more information, see Performance impacts in the IBM QRadar Network Insights *Installation Guide*.

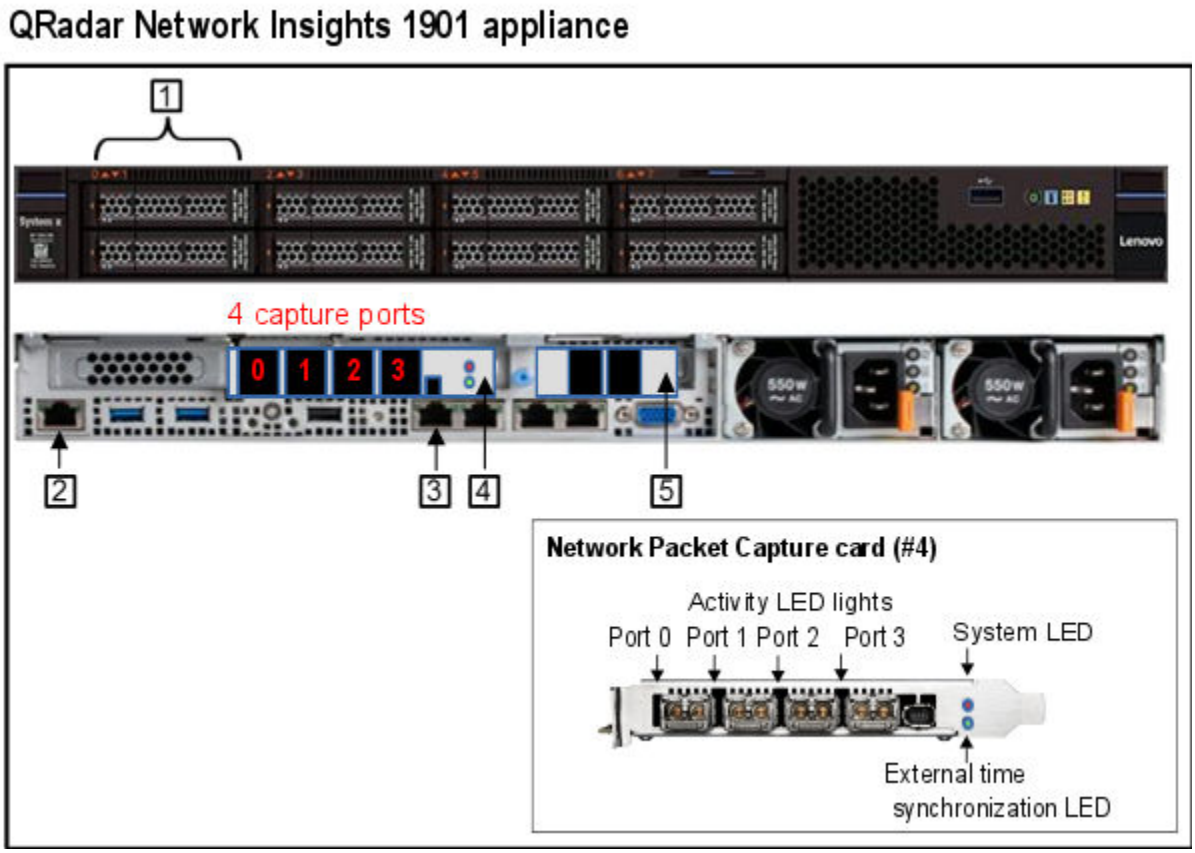


Figure 24. Back panel of the QRadar Network Insights 1901 appliance

Table 47. Legend for use with the QRadar Network Insights 1901 image	
Label	**Description**
1	QRadar Firmware Storage
2	1 x RJ-45 10/100/1000 Mb Ethernet systems management (IMM) port
3	Management ports (1 GbE TX)
4	Network Packet Capture (SFP)
5	Management ports (10 GbE SFP+)

Note: Only the Network Packet Capture card [4] can be used for capturing network packet data.

For battery removal steps, see Removing the coin-cell battery (also called CMOS battery) (http://www-01.ibm.com/support/knowledgecenter/api/redirect/systemx/documentation/index.jsp?topic=/com.lenovo.sysx.8871.doc/t_removing_system_battery.html)

For more information about the QRadar Network Insights 1901, including front and back panel diagrams, see IBM System X3550 M5 (https://lenovopress.com/lp0067-lenovo-system-x3550-m5-machine-type-8869).

QRadar Network Insights 1901-C

The IBM QRadar Network Insights 1901-C (MTM 4654-F6Y) appliance provides detailed analysis of network flows to extend the threat detection capabilities of IBM QRadar.

With four 1G capture ports on a Napatech card, the QRadar Network Insights 1901-C appliance provides the same capabilities as the QRadar Network Insights 1920 appliance but on a lower-price hardware platform that is designed for 1 Gbps network connectivity.

Table 48. QRadar Network Insights 1901-C specifications

Description	**Value**
CPU	2 x Xeon Gold 5118 12C 2.3 GHz 16 MB Cache 3.20 GHz 105 W
Network capture transceivers	4 x 1 G TX RJ-45 Transceivers (Avago ABCU-5710RZ or ABCU-5740RZ) 4 x 1 G SX LC Transceivers (Avago AFBR-5715PZ) Use these transceivers with the network packet capture card, labeled as [5] in the appliance diagram.
Network management transceivers	2 x 10 GbE Short Range SFP+ The transceivers might have one of the following part numbers: • Avago AFBR-709SMZ-IB8 • Finisar FTLX8571D3BCL-BN • BNT BN-CKM-SP-SR Use these transceivers with the 2 x 10 GbE SFP+ ports, labeled as [3] in the appliance diagram
Ports	4 x 1 Gb Ethernet ports 1 x RJ-45 10/100/1000 Mb Ethernet systems management (IMM) port 2 x 10 GbE SFP+ ports 4 x Network capture ports (SFP)
Memory	64 GB, 4 x 16 GB
Storage	2 x 240 GB SATA 2.5" SSD, 240 GB Total (RAID1)
Traffic	1 Gbps
Power supply	Dual redundant 750 W AC
Unit weight	48.5 lbs
Physical dimensions	31.1 inches deep x 17.1 inches wide x 1.7 inches high

The following image is of the QRadar Network Insights 1901-C appliance.

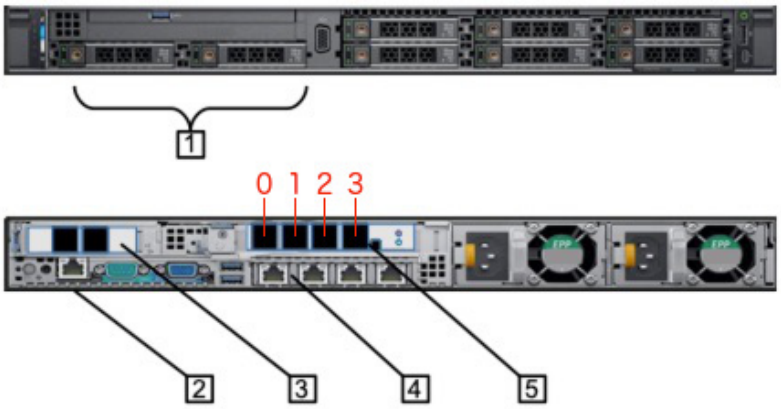


Figure 25. Front and rear panel of the QRadar Network Insights 1901-C appliance

Table 49. Legend for use with the QRadar Network Insights 1901-C image	
Label	**Description**
1	QRadar firmware storage
2	1 x RJ-45 10/100/1000 Mb Ethernet systems management (IMM) port
3	Management ports (10 GbE SFP+)
4	Management ports (1 GbE TX)
5	Network packet capture (SFP) Ports are numbered 0, 1, 2, 3, from left to right.

For information about battery replacement, see *Dell EMC PowerEdge R640 Installation and Service Manual* (https://topics-cdn.dell.com/pdf/poweredge-r640_owners-manual_en-us.pdf).

QRadar Network Insights 1910

The IBM QRadar Network Insights 1910 (MTM 4412-F5Y) appliance offers 1 Gbps and 10 Gbps connectivity in a smaller, lower-cost appliance for deployments that require 10 Gbps connectivity but don't require the same level of processing or performance that is found in the more powerful 1920 appliance.

Table 50. QRadar Network Insights 1910 overview	
Description	**Value**
CPU	1 x E5-2680 v4 2.4 GHz 14C 2.4 GHz 35 MB Cache 2400 MHz 120 W
Network capture transceivers	• 4 x 10 Gb Short Range Fiber Transceivers (Avago AFBR-703SDZ or AFBR-709SMZ) • 4 x 10 Gb Long Range Fiber Transceivers (Avago AFCT-739SMZ) Use these transceivers with the 4 x Network Packet Capture (SFP+) ports, labeled as [4] in the appliance diagram

Table 50. QRadar Network Insights 1910 overview (continued)	
Description	**Value**
Network management transceivers	2 x 10 GbE Short Range SFP+ Lenovo PN 46C3446-5053 The transceiver may have one of the following part numbers: • Avago AFBR-709SMZ-IB8 • Finisar FTLX8571D3BCL-BN • BNT BN-CKM-SP-SR Use these transceivers with the 2 x 10 GbE SFP+ ports, labeled as [5] in the appliance diagram
Ports	4 x 1 Gb Ethernet ports 2 x 10 GbE SFP+ ports 1 x RJ-45 10/100/1000 Mb Ethernet systems management (IMM) port 4 x Network Packet Capture (SFP+) ports
Memory	64 GB, 4 x 16 GB
Storage	2 x 240 GB SATA 2.5" SSD, 480 GB Total (RAID1) OR 2 x 200 GB SATA 2.5" SSD, 400 GB Total (RAID1) The storage is labeled as [1] in the appliance diagram.
Traffic rate	10 Gbps
Power supply	Dual redundant 750 W AC
Unit weight	31 lbs
Physical dimensions	28.9 inches deep x 17.1 inches wide x 1.7 inches high

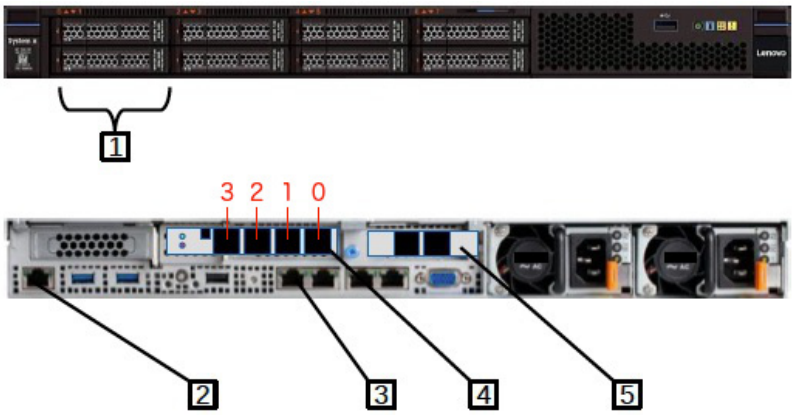


Figure 26. QRadar Network Insights 1910

Table 51. Legend for use with the QRadar Network Insights 1910 image	
Label	**Description**
1	QRadar firmware storage
2	1 x RJ-45 10/100/1000 Mb Ethernet systems management (IMM) port

Table 51. Legend for use with the QRadar Network Insights 1910 image (continued)	
Label	**Description**
3	Management ports (1 GbE TX)
4	Network Packet Capture ports (SFP+)
5	Management ports (10 GbE SFP+)

QRadar Network Insights 1910-C

The IBM QRadar Network Insights 1910-C (MTM 4654-Q9C) appliance offers 1 Gbps and 10 Gbps connectivity in a smaller, lower-cost appliance for deployments that require 10 Gbps connectivity but don't require the same level of processing or performance that is found in the more powerful 1920 appliance.

Table 52. QRadar Network Insights 1910-C specifications	
Description	**Value**
CPU	2 x Xeon Gold 5118 12C 2.3 GHz 16 MB Cache 3.20 GHz 105 W
Network Capture Transceivers	4 x 1 G TX RJ-45 Transceivers (Avago ABCU-5710RZ or ABCU-5740RZ) 4 x 1 G SX LC Transceivers (Avago AFBR-5715PZ) Use these transceivers with the network packet capture card, labeled as [5] in the appliance diagram.
Network Management Transceivers	2 x 10 GbE Short Range SFP+ The transceivers might have one of the following part numbers: • Avago AFBR-709SMZ-IB8 • Finisar FTLX8571D3BCL-BN • BNT BN-CKM-SP-SR Use these transceivers with the 2 x 10 GbE SFP+ ports, labeled as [3] in the appliance diagram
Network ports	Network Packet Capture (SFP+) ports 4 x 1 Gb Ethernet ports 1 x RJ-45 10/100/1000 Mb Ethernet systems management (IMM) port 2 x 10 GbE SFP+ ports
Memory	64 GB, 4 x 16 GB
Storage	2 x 240 GB SATA 2.5" SSD, 240 GB Total (RAID1)
Traffic	10 Gbps
Power supply	Dual redundant 750 W AC
Unit weight	48.5 lbs
Physical dimensions	31.3 inches deep x 17.1 inches wide x 1.7 inches high

The following image is of the QRadar Network Insights 1910-C appliance.

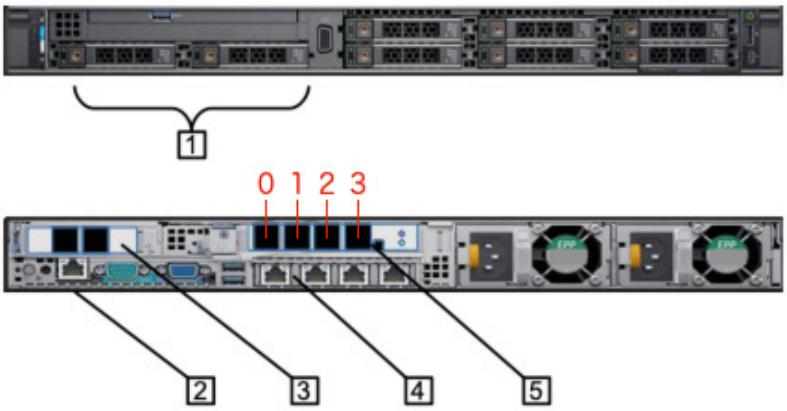


Figure 27. Front and rear panel of the QRadar Network Insights 1910-C appliance

Table 53. Legend for use with the QRadar Network Insights 1910-C image	
Label	**Description**
1	QRadar firmware storage
2	1 x RJ-45 10/100/1000 Mb Ethernet systems management (IMM) port
3	Management ports (10 GbE SFP+)
4	Management ports (1 GbE TX)
5	Network Packet Capture (SFP+) Ports are numbered 0, 1, 2, 3, from left to right.

For information about battery replacement, see *Dell EMC PowerEdge R640 Installation and Service Manual* (https://topics-cdn.dell.com/pdf/poweredge-r640_owners-manual_en-us.pdf).

QRadar Network Insights 1920

The IBM QRadar Network Insights 1920 (MTM 4412-F3F) appliance provides detailed analysis of network flows to extend the threat detection capabilities of IBM QRadar.

The appliance has two Napatech cards, each with four ports. By default, the four ports on the first network capture card are configured for inbound traffic from the network tap. If the appliance is included in a stack, the ports are reconfigured for 2 inbound ports and 2 outbound ports. For more information about cabling stacked appliances, see the IBM QRadar Network Insights *Installation Guide*.

The second Napatech card is cabled internally for load balancing and cannot not be used. If you use these ports when you cable the appliance, you do not get any data.

The following table shows the hardware information and requirements for the IBM QRadar Network Insights 1920 (MTM 4412-F3F) appliance:

Table 54. QRadar Network Insights 1920 overview	
Description	**Value**
CPU	2 x E5-2680 v4 14C 2.4 GHz 35 MB 2400 MHz 120W

Table 54. QRadar Network Insights 1920 overview (continued)	
Description	**Value**
Network capture transceivers	2 x 10 Gb Short Range fiber Transceivers (Avago AFBR-703SDZ or AFBR-709SMZ) 2 x 1 G TX RJ-45 Transceivers (Avago ABCU-5710RZ or ABCU-5740RZ) 2 x 1 G SX LC Transceivers (Avago AFBR-5715PZ) Use these transceivers with the network packet capture card, labeled as [2] in the appliance diagram.
Network management transceivers	2 x 10 GbE Short Range SFP+ The transceivers can have one of the following part numbers: • Avago AFBR-709SMZ-IB8 • Finisar FTLX8571D3BCL-BN • BNT BN-CKM-SP-SR Use these transceivers with the 2 x 10 GbE SFP+ ports, labeled as [4] in the appliance diagram.
Ports	Network Packet Capture (SFP/SFP+) ports (Model NT40E3-4) 4 x 1 Gb Ethernet ports 1 x RJ-45 10/100/1000 Mb Ethernet systems management (IMM) port 2 x 10 GbE SFP+ ports
Storage	2 x 240 GB SATA 2.5" SSD, 480 GB Total (RAID1) OR 2 x 200 GB SATA 2.5" SSD, 400 GB Total (RAID1) The storage is labeled as [1] in the appliance diagram.
Memory	128 GB (8 x 16 GB DDR4 2400 MHz)
Traffic	10 Gbps
Power	Dual redundant 900-Watt AC power supply
Dimensions	29.5 inches deep x 17.6 inches wide (19 inches with EIA) x 3.4 inches high

System performance of QRadar Network Insights appliances varies depending on the exact configuration and tuning of the system components. It is influenced not only by hardware, but also factors such as the search, extraction criteria, and the amount of network data. For more information, see Performance impacts in the IBM QRadar Network Insights *Installation Guide*.

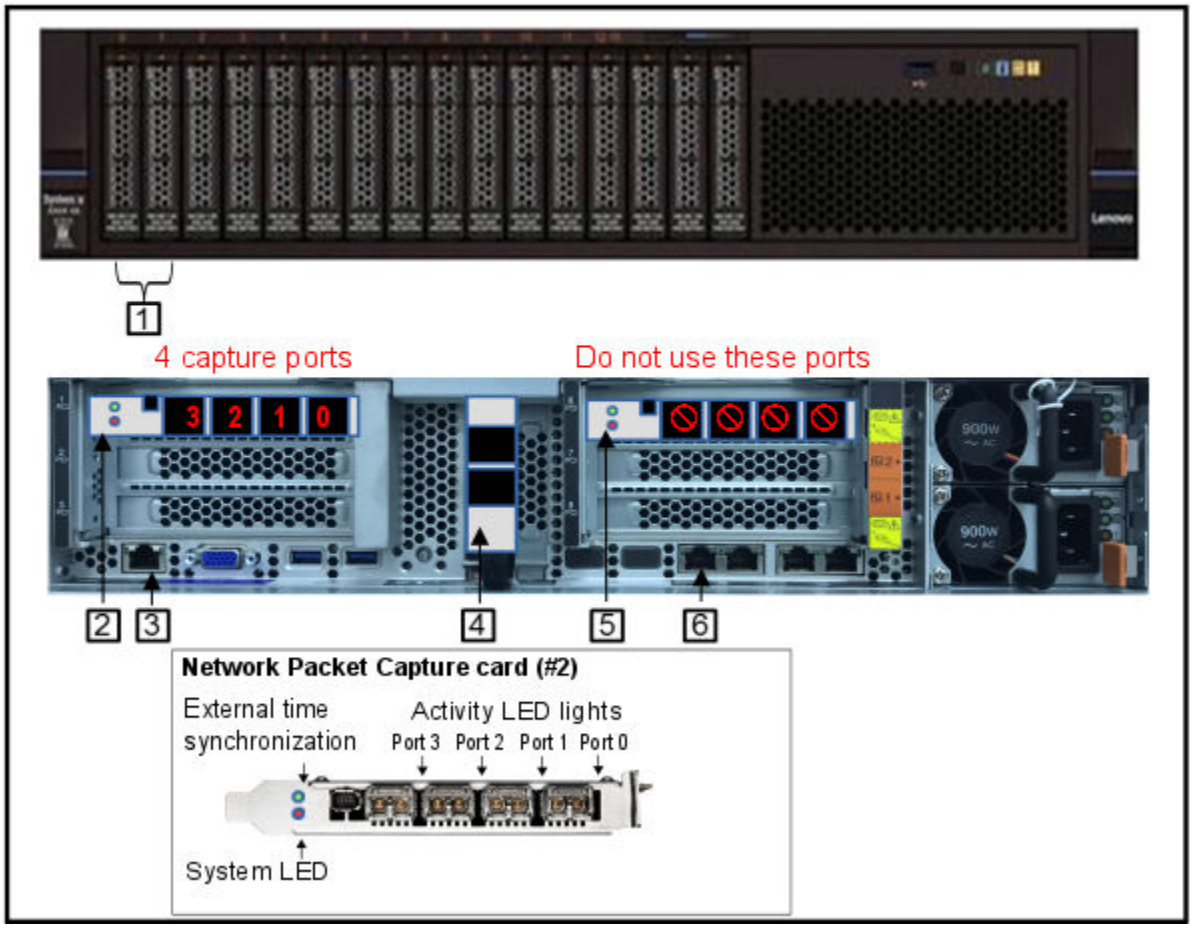


Figure 28. Back panel of the QRadar Network Insights 1920 appliance

Table 55. Legend for use with the QRadar Network Insights 1920 image	
Label	**Description**
1	QRadar Firmware Storage
2	Network Packet Capture (SFP/SFP+)
3	IMM Port (1GbE TX)
4	Management ports (10 GbE SFP+)
5	Cabled internally. Do not use these ports.
6	Management ports (1 GbE TX)

For battery removal steps, see Removing the coin-cell battery (also called CMOS battery) (http://publib.boulder.ibm.com/infocenter/systemx/documentation/index.jsp?topic=/com.lenovo.sysx.8871.doc/t_removing_system_battery.html)

For more information about the front panel, see Front view (http://publib.boulder.ibm.com/infocenter/systemx/documentation/index.jsp?topic=/com.lenovo.sysx.8871.doc/c_front_view.html).

For more information about the back panel, see Rear view (http://publib.boulder.ibm.com/infocenter/systemx/documentation/index.jsp?topic=/com.lenovo.sysx.8871.doc/c_rear_view.html).

For more information, you can also see System x3650 M5 (https://lenovopress.com/lp0068-lenovo-system-x3650-m5-machine-type-8871.html).

QRadar Network Insights 1920-C

The IBM QRadar Network Insights 1920-C (MTM 4654-F4F) appliance provides detailed analysis of network flows to extend the threat detection capabilities of IBM QRadar.

The appliance has two Napatech cards, each with four ports. By default, the four ports on the first network capture card are configured for inbound traffic from the network tap. If the appliance is included in a stack, the ports are reconfigured for 2 inbound and 2 outbound. For more information about cabling stacked appliances, see the IBM QRadar Network Insights *Installation Guide*.

The second Napatech card is cabled internally for load balancing and cannot not be used. If you use these ports when you cable the appliance, you do not get any data.

The following table shows the hardware information and requirements for the IBM QRadar Network Insights 1920-C (MTM 4654-F4F) appliance.

Table 56. QRadar Network Insights 1920-C specifications

Description	**Value**
CPU	2 x Xeon Gold 6132 14C 2.6 GHz 19 MB Cache 3.70 GHz 140 W
Network capture transceivers	2 x 10 Gb Short Range fiber Transceivers (Avago AFBR-703SDZ or AFBR-709SMZ) 2 x 1 G TX RJ-45 Transceivers (Avago ABCU-5710RZ or ABCU-5740RZ) 2 x 1 G SX LC Transceivers (Avago AFBR-5715PZ) Use these transceivers with the network packet capture card, labeled as [2] in the appliance diagram.
Network management transceivers	2 x 10 GbE Short Range SFP+ The transceivers can have one of the following part numbers: • Avago AFBR-709SMZ-IB8 • Finisar FTLX8571D3BCL-BN • BNT BN-CKM-SP-SR Use these transceivers with the 2 x 10 GbE SFP+ ports, labeled as [3] in the appliance diagram.
Ports	Network Packet Capture (SFP/SFP+) port (Model NT40E3-4) 4 x 1 Gb Ethernet ports 1 x RJ-45 10/100/1000 Mb Ethernet systems management (IMM) port 2 x 10 Gbps SFP+ management ports
Memory	128 GB, 8 x 16 GB
Storage	2 x 240 GB SATA 2.5" SSD, 240 GB Total (RAID1)
Traffic rate	10 Gbps
Power supply	Dual redundant 750 W AC
Unit weight	73 lbs
Physical dimensions	29.0 inches deep x 17.1 inches wide x 3.4 inches high

The following image is of the QRadar Network Insights 1920-C appliance.

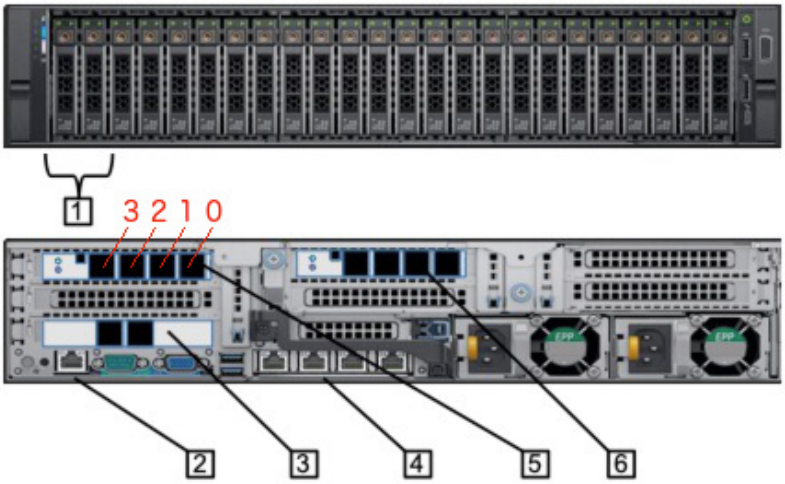


Figure 29. Front and back panel of the QRadar Network Insights 1920-C appliance

Table 57. Legend for use with the QRadar Network Insights 1920-C image	
Label	**Description**
1	QRadar firmware storage
2	1 x RJ-45 10/100/1000 Mb Ethernet systems management (IMM) port
3	Management ports (10 GbE SFP+)
4	Management ports (1 GbE TX)
5	Network Packet Capture (SFP/SFP+) Ports are numbered 3, 2, 1, 0, from left to right.
6	Do not use these ports

For information about battery replacement, see *Dell EMC PowerEdge R740 Installation and Service Manual* (https://topics-cdn.dell.com/pdf/poweredge-r740_owners-manual_en-us.pdf).

QRadar Incident Forensics

Use the IBM QRadar Incident Forensics appliance (MTM 4412-F1A) to retrace the step-by-step actions of a potential attacker, and quickly and easily conduct an in-depth forensics investigation of suspected malicious network security incidents.

View hardware information and requirements for the QRadar Incident Forensics appliance in the following table:

Table 58. Incident Forensics appliance specifications	
Description	**Value**
CPU	2 x E5-2650 v4 12C 2.2 GHz 30 MB 2400 MHz 105W

Table 58. Incident Forensics appliance specifications (continued)	
Description	**Value**
Network management transceiver	2 x 10 GbE Short Range SFP+ The transceivers might have one of the following part numbers: • Avago AFBR-709SMZ-IB8 • Finisar FTLX8571D3BCL-BN • BNT BN-CKM-SP-SR Use these transceivers with the 2 x 10 GbE SFP+ ports, labeled as [3] in the appliance diagram.
Ports	3 x 10/100/1000 Base-T network ports 1 x RJ-45 10/100/1000 Mb Ethernet systems management (IMM) port 1 x 10/100/1000 Base-T integrated remote system management port 2 x 10 GbE SFP+ ports
Memory	128 GB, 8 x16 GB truDDR4 2400 MHz LP RDIMM
Storage	12 x 3.5 inches 6 TB SAS 7.2 K rpm, 60 TB total (RAID6)
Power supply	System x 900W High Efficiency Platinum AC Power Supply
Dimensions	31.5 inches deep x 17.5 inches wide x 3.4 inches high

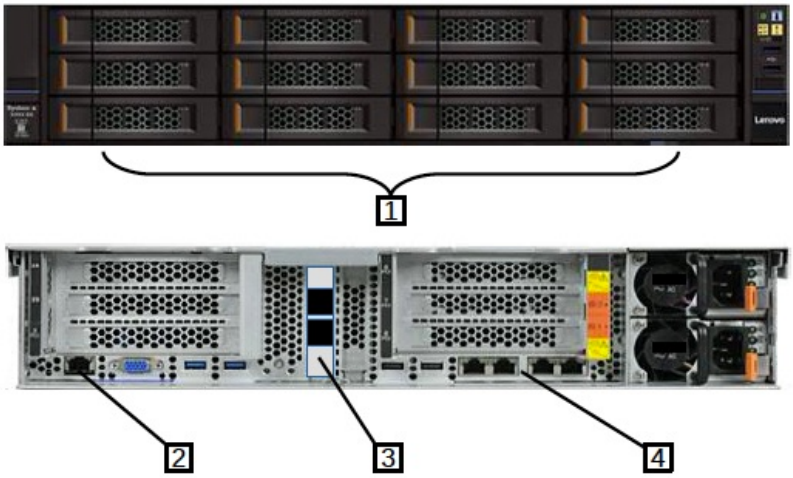


Figure 30. QRadar Incident Forensics

Table 59. Legend for use with the QRadar Incident Forensics image	
Label	**Description**
1	Event data storage
2	1 x RJ-45 10/100/1000 Mb Ethernet systems management (IMM) port
3	10 GbE SFP+ management ports
4	Management ports (1 GbE TX)

For more information about the front panel, see Front view (http://publib.boulder.ibm.com/infocenter/systemx/documentation/index.jsp?topic=/com.lenovo.sysx.8871.doc/c_front_view.html).

For more information about the back panel, see Rear view (http://publib.boulder.ibm.com/infocenter/systemx/documentation/index.jsp?topic=/com.lenovo.sysx.8871.doc/c_rear_view.html).

For more information, you can also see System x3650 M5 (https://lenovopress.com/lp0068-lenovo-system-x3650-m5-machine-type-8871.html).

QRadar Incident Forensics-C

Use the IBM QRadar Incident Forensics-C appliance (MTM 4654-F2A) to retrace the step-by-step actions of a potential attacker, and to quickly and easily conduct an in-depth forensics investigation of suspected malicious network security incidents.

The following table describes hardware information and requirements for the QRadar Incident Forensics-C appliance:

Table 60. QRadar Incident Forensics-C specifications

Description	**Value**
CPU	R640 XL, 2 x Xeon Gold 5118, 2.3 GHz 16 MB Cache 3.20 GHz 105 W
Network management transceivers	2 x 10 GbE Short Range SFP+ The transceivers can have one of the following part numbers: • Avago AFBR-709SMZ-IB8 • Finisar FTLX8571D3BCL-BN • BNT BN-CKM-SP-SR Use these transceivers with the 2 x 10 GbE SFP+ ports, labeled as [3] in the appliance diagram.
Ports	4 x 1 Gb Ethernet ports 1 x RJ-45 10/100/1000 Mb Ethernet systems management (IMM) port 2 x 10 GbE SFP+ management ports
Memory	128 GB, 8 x 16 GB
Storage	12 x 8 TB 7.2 K 12 Gbps 512e 3.5” NLSAS, 80 TB total (RAID6)
Power supply	Dual redundant 1100 W AC
Unit weight	73 lbs
Physical dimensions	29.0 inches deep x 17.1 inches wide x 3.4 inches high

The following image is of the QRadar Incident Forensics-C appliance.

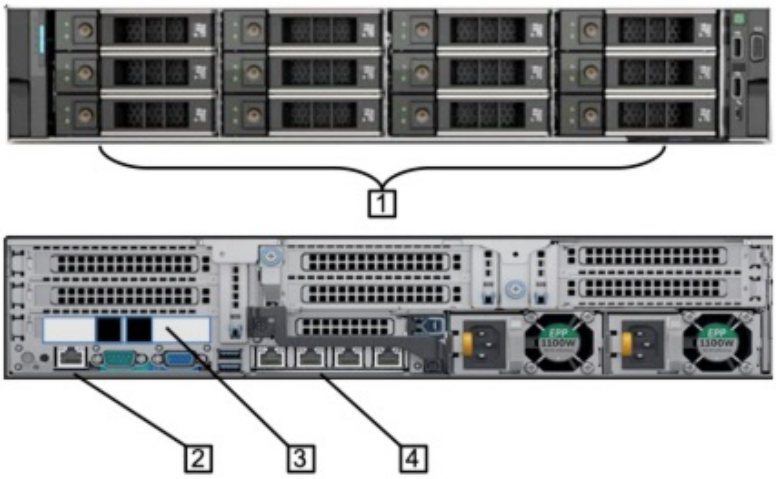


Figure 31. Front and rear panel of theQRadar Incident Forensics-C appliance

Table 61. Legend for use with the QRadar Incident Forensics-C image	
Label	**Description**
1	Event data storage
2	1 x RJ-45 10/100/1000 Mb Ethernet systems management (IMM) port
3	10 Gbps SFP+ management ports
4	Management ports (1 GbE TX)

For information about battery replacement, see *Dell EMC PowerEdge R740 Installation and Service Manual* (https://topics-cdn.dell.com/pdf/poweredge-r740_owners-manual_en-us.pdf).

QRadar Network Packet Capture

IBM QRadar Network Packet Capture (MTM 4412-F2C) offers an optional Network Packet Capture appliance to store and manage data that is used by QRadar Incident Forensics when no other network packet capture (Network PCAP) device is deployed. Any number of these appliances can be installed as a tap on a network or sub-network to collect the raw packet data.

View hardware information and requirements for QRadar Network Packet Capture in the following table:

Table 62. QRadar Network Packet Capture overview	
Description	**Value**
CPU	2 x E5-2680 v4 14C 2.4GHz 35MB Cache 2400MHz 120W
Network capture transceivers	4 x SR 10 Gb SFP+ 4 x TX 1Gb SFP 4 x SX 1Gb SFP Use these transceivers with the network packet capture card, labeled as [7] in the appliance diagram.

Table 62. QRadar Network Packet Capture overview (continued)	
Description	**Value**
Network management transceiver	2 x 10 GbE Short Range SFP+ The transceivers can have one of the following part numbers: • Avago AFBR-709SMZ-IB8 • Finisar FTLX8571D3BCL-BN • BNT BN-CKM-SP-SR Use these transceivers with the 2 x 10 GbE SFP+ ports, labeled as [5] in the appliance diagram.
Ports	4 x 1 Gb Ethernet ports 1 x RJ-45 10/100/1000 Mb Ethernet systems management (IMM) port 2 x 10 Gbps SFP+ management ports 4 x Network packet capture (SFP/SFP+) ports (Model NT40E3-4)
Memory	128 GB (8 x 16 GB) DDR4 RDIMM
Storage	12 x 3.5 inch 6 TB NLSAS 7.2 K rpm, 60 TB total (RAID5) 2 x 2.5 inch 1TB NLSAS 7.2 K rpm, 1 TB total (RAID1)
Power supply	Dual redundant 900 W AC
Dimensions	31.5 inches deep x 17.5 inches wide (19 inches with EIA) x 3.4 inches high

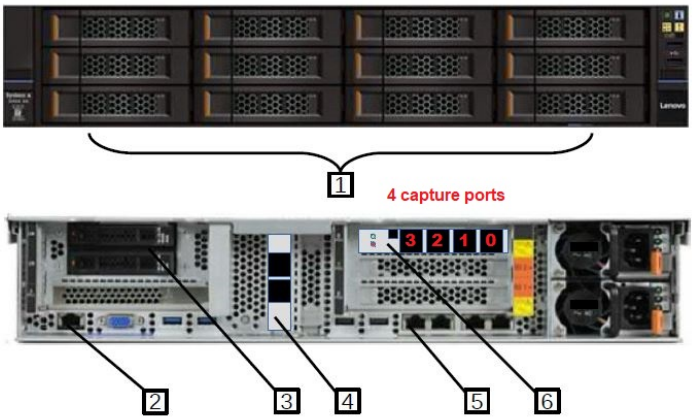


Figure 32. QRadar Network Packet Capture

Table 63. Legend for use with the QRadar Network Packet Capture image	
Label	**Description**
1	Event data storage
2	1 x RJ-45 10/100/1000 Mb Ethernet systems management (IMM) port
3	QRadar firmware storage
4	10 Gbps SFP+ management ports
5	Management ports (1 GbE TX)

Table 63. Legend for use with the QRadar Network Packet Capture image (continued)	
Label	**Description**
6	Network packet capture (SFP/SFP+)

For battery removal steps, see Removing the coin-cell battery (also called CMOS battery) (http://publib.boulder.ibm.com/infocenter/systemx/documentation/index.jsp?topic=/com.lenovo.sysx.8871.doc/t_removing_system_battery.html)

For more information about the front panel, see Front view (http://publib.boulder.ibm.com/infocenter/systemx/documentation/index.jsp?topic=/com.lenovo.sysx.8871.doc/c_front_view.html).

For more information about the back panel, see Rear view (http://publib.boulder.ibm.com/infocenter/systemx/documentation/index.jsp?topic=/com.lenovo.sysx.8871.doc/c_rear_view.html).

For more information, you can also see System x3650 M5 (https://lenovopress.com/lp0068-lenovo-system-x3650-m5-machine-type-8871.html).

QRadar Network Packet Capture Direct Attached Storage

New in 7.4.1 As an option you can add the QRadar Network Packet Capture Direct Attached Storage (4563-D1S) appliance to the IBM QRadar Network Packet Capture appliance to increase the storage capacity. You can manage both the internal and external storage as a single interface. This helps reduce resource load on the system and enables easier navigation. The QRadar Network Packet Capture Direct Attached Storage appliance is based on the Lenovo D1212.

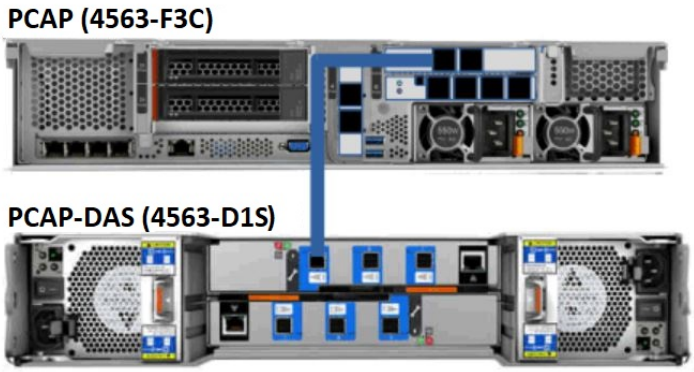
Note: You must use the Lenovo QRadar Network PCAP Direct Attached Storage appliance with the Lenovo QRadar Network Packet Capture appliance.

Table 64. QRadar Network PCAP Direct Attached Storage specifications	
Description	**Value**
Ports	3 x 12 Gb Mini-SAS 2 x 10/100 MbE management
Storage	12 x 8 TB 3.5” RAID 5 (88 TB)
Power supply	2 x 580 W AC
Dimensions	24.8 inches deep x 17.4 inches wide x 3.4 inches high

The following image is of the QRadar Network PCAP Direct Attached Storage appliance.

Figure 33. Front and rear panel of the QRadar Network PCAP Direct Attached Storage appliance

The QRadar Network Packet Capture appliance can have up to eight QRadar Network Packet Capture Direct Attached Storage (4563-D1S) storage units connected in a daisy chain configuration. The following image is of the QRadar Network Packet Capture appliance with a QRadar Network PCAP Direct Attached Storage appliance that is connected showing the wiring configuration.



The QRadar Network Packet Capture appliance can capture up to 10 Gbps. Adding QRadar Network PCAP Direct Attached Storage appliances to your Lenovo QRadar Network Packet Capture does not increase the capture rate.

QRadar Network Packet Capture-C

QRadar Network Packet Capture-C (MTM 4654-F3C) offers an optional Network Packet Capture appliance to store and manage data that is used by QRadar Incident Forensics when no other network packet capture (Network PCAP) device is deployed. Any number of these appliances can be installed as a tap on a network or sub-network to collect the raw packet data.

View hardware information for QRadar Network Packet Capture-C in the following table:

Table 65. QRadar Network Packet Capture-C specifications

Description	Value
CPU	2 x Xeon Gold 6132 14C 2.6 GHz 19 MB Cache 3.70 GHz 140 W

Table 65. QRadar Network Packet Capture-C specifications (continued)	
Description	**Value**
Network capture transceivers	4 x SR 10 Gb SFP+ 4 x TX 1Gb SFP 4 x SX 1Gb SFP Use these transceivers with the network packet capture card, labeled as [6] in the appliance diagram.
Network management transceivers	2 x 10 GbE Short Range SFP+ The transceivers can have one of the following part numbers: • Avago AFBR-709SMZ-IB8 • Finisar FTLX8571D3BCL-BN • BNT BN-CKM-SP-SR Use these transceivers with the 2 x 10 GbE SFP+ ports, labeled as [3] in the appliance diagram.
Ports	4 x 1 Gb Ethernet ports 1 x RJ-45 10/100/1000 Mb Ethernet systems management (IMM) port 2 x 10 Gbps SFP+ management ports 2 x Direct Attached Storage (DAS) ports 4 x Network packet capture (SFP/SFP+) ports (Model NT40E3-4)
Memory	128 GB, 8 x 16 GB
Storage	12 x 8 TB 7.2 K 12 Gbps NLSAS 3.5", 80 TB total (RAID5) 2 x 1 TB 7.2 K 12 Gbps NLSAS 2.5", 1 TB total (RAID1)
Power supply	Dual redundant 1100 W AC
Unit weight	73 lbs
Physical dimensions	29.0 inches deep x 17.1 inches wide x 3.4 inches high

The following image is of the QRadar Network Packet Capture-C appliance.

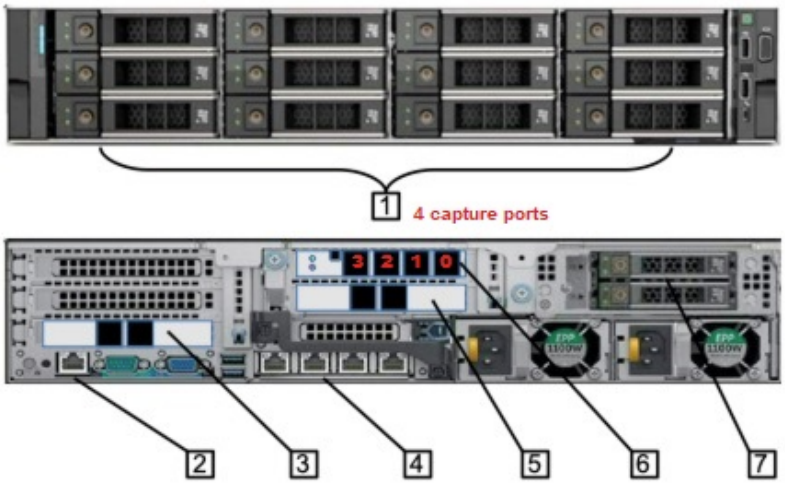


Figure 34. Front and rear panel of the QRadar Network Packet Capture-C

Table 66. Legend for use with the QRadar Network Packet Capture-C image	
Label	**Description**
1	Packet capture storage
2	1 x RJ-45 10/100/1000 Mb Ethernet systems management (IMM) port
3	10 Gbps SFP+ management ports
4	Management ports (1 GbE TX)
5	External RAID DAS ports
6	Network packet capture (SFP/SFP+)
7	QRadar firmware storage

For information about battery replacement, see *Dell EMC PowerEdge R740 Installation and Service Manual* (https://topics-cdn.dell.com/pdf/poweredge-r740_owners-manual_en-us.pdf).

Chapter 4. QRadar M4 appliance overview

Review information about IBM QRadar to understand hardware and license requirements.

Review this overview of QRadar appliances, including capabilities, and license limitations.

IBM QRadar appliances are certified to support a certain maximum events per second (EPS) rate. Maximum EPS depends on the type of data that is processed, system configuration, and system load. For more information, see QRadar maximum EPS certification methodology.

Integrated Management Module

The Integrated Management Module (IMM) is a management module that is used for systems-management functions.

On the back panel of each appliance type, the serial connector and Ethernet connectors can be managed by using the Integrated Management Module (IMM). You can configure the IMM to share an Ethernet port with the IBM QRadar management interface; however, you can configure the IMM in dedicated mode to reduce the risk of losing the IMM connection when the appliance is restarted. To configure the IMM, you must access the System BIOS settings by pressing the F1 key when the IBM splash screen is displayed. For further instructions on how to configure the IMM, see the *Integrated Management Module User's Guide* that comes with your appliance.

QRadar xx05

Use the IBM QRadar xx05 (MTM 4380-Q1E) for various appliance types in your deployment.

The QRadar xx05 can be used for the following appliances:

- QRadar Event Processor 1605
- QRadar Flow Processor 1705
- QRadar 1805
- QRadar 3105 (All-in-One)
- QRadar 3105 (Console)
- QRadar Log Manager 1605
- QRadar Log Manager 3105 (All-in-One)
- QRadar Log Manager 3105 Console
- QRadar 1400 Data Node
- QRadar Vulnerability Manager
- QRadar Risk Manager

View hardware information and requirements for the QRadar xx05 in the following table:

Table 67. QRadar xx05

Description	Value
Maximum capacity	QRadar Event Processor 1605 20,000 EPS QRadar Flow Processor 1705 1,200,000 FPM QRadar 1805 200,000 FPM, 5,000 EPS QRadar 3105 (All-in-One) 200,000 FPM, 5,000 EPS QRadar Vulnerability Manager up to 32,768 assets

Table 67. QRadar xx05 (continued)	
Description	**Value**
Interfaces	Two 10/100/1000 Base-T network monitoring interfaces One 10/100/1000 Base-T QRadar management interface One 10/100/1000 Base-T integrated management module interface Two 10 Gbps SFP + ports
Memory	64 GB 8x 8 GB 1600 MHz RDIMM
Storage	9 x 3.5 inch 1 TB 7.2 K rpm NL SAS, 9 TB total, 5.5 TB usable (RAID 6) QRadar 1400 Data Node 9 x 3.5 inch 1 TB 7.2 K rpm NL SAS, 9 TB total, 6.1 TB usable (RAID 6)
Power supply	Dual Redundant 750 W AC Power Supply
Dimensions	29.5 inches deep x 17.7 inches wide x 2.4 inches high
Included components	Event Collector Event Processor Flow Processor Internal storage for events and flows QRadar Data Node appliance QRadar Vulnerability Manager QRadar Risk Manager

The QRadar 3105 (All-in-One) requires external QRadar QFlow Collectors for layer 7 network activity monitoring.

For more information about IBM QRadar M4 Consoles, Processors and Data Nodes, including front and back panel diagrams, see IBM System X3650 M4 BD (https://lenovopress.com/tips1102-system-x3650-m4-bd).

QRadar xx28

Use the IBM QRadar xx28 (MTM 4380-Q2E) for various appliance types in your deployment.

The QRadar xx28 can be used for the following appliances:

- QRadar Event Processor 1628
- QRadar Flow Processor 1728
- QRadar Flow Processor 1828
- QRadar 3128 (All-in-One)
- QRadar 3128 (Console)
- QRadar Log Manager 1628
- QRadar Log Manager 3128 (All-in-One)
- QRadar Log Manager 3128 (Console)
- QRadar 1400 Data Node

Note: For QRadar xx28 appliances, you are responsible for acquiring the proper transceivers for your network.

View hardware information and requirements for the QRadar xx28 in the following table:

Table 68. QRadar xx28	
Description	**Value**
Maximum capacity	QRadar Event Processor 1628 40,000 EPS QRadar Flow Processor 1728 1,200,000 FPM QRadar Flow Processor 1828 300,000 FPM, 15,000 EPS QRadar 3128 (All-in-One) 300,000 FPM, 15,000 EPS
Interfaces	One 2-port Emulex 8Gbps FC Two 10/100/1000 Base-T network monitoring interfaces One 10/100/1000 Base-T QRadar management interface One 10/100/1000 Base-T integrated management module interface Two 10 Gbps SFP + ports Packet capture - Four 10 GBps SFP + ports
Memory	128 GB, 8 x 16 GB 1866 MHz RDIMM8
Storage	12 x 3.5 inch 4 TB SAS 7.2 K rpm, 48 TB total, 34 TB usable (RAID 6) QRadar 1400 Data Node 12 x 3.5 inch 4 TB SAS 7.2 K rpm, 48 TB total, 39 TB usable (RAID 6)
Power supply	Dual Redundant 900 W AC Power Supply
Dimensions	29.5 inches deep x 17.6 inches wide x 3.4 inches high
Included components	Event Collector Event Processor Flow Processor Internal storage for events and flows QRadar Data Node appliance

The QRadar 3128 (All-in-One) requires external QRadar QFlow Collectors for layer 7 network activity monitoring.

For more information about IBM QRadar M4 Consoles, Processors and Data Nodes, including front and back panel diagrams, see IBM System X3650 M4 BD (https://lenovopress.com/tips1102-system-x3650-m4-bd).

QRadar xx28-C

Use the IBM QRadar xx28-C (MTM 4380-Q1F) for various appliance types in your deployment.

IBM QRadar xx28-C appliances are manufactured by Dell, and can be used for the following appliances:

- QRadar Event Processor 1628-C
- QRadar Flow Processor 1728-C
- QRadar Flow Processor 1828-C
- QRadar 3128-C (All-in-One)
- QRadar 3128-C (Console)
- QRadar Log Manager 1628-C
- QRadar Log Manager 3128-C (All-in-One)

- QRadar Log Manager 3128-C (Console)
- QRadar Risk Manager
- QRadar Vulnerability Manager
- QRadar Incident Forensics
- QRadar 1400-C Data Node

QRadar xx28-C appliances are TAA compliant. You can also use the xx28-C appliances for FIPS compliance.

Important: To make an xx28-C appliance FIPS compliant, the QRadar release must be FIPS compliant, and your appliance must have the required physical security. For more information about physical security, see the *IBM Security QRadar Version 7.2.5 FIPS 140-2 Installation Guide*. QRadar Incident Forensics is not FIPS compliant.

Table 69. QRadar xx28-C

Description	**Value**
Maximum capacity	QRadar Event Processor 1628-C 40,000 EPS QRadar Flow Processor 1728-C 1,200,000 FPM QRadar Flow Processor 1828-C 300,000 FPM, 15,000 EPS QRadar 3128-C (All-in-One) 300,000 FPM, 15,000 EPS
Interfaces	One 2-port Emulex 8Gbps FC Three 10/100/1000 Base-T network monitoring interfaces One 10/100/1000 Base-T QRadar management interface One 10/100/1000 Base-T integrated remote system management interface Two 10 Gbps SFP + ports
Memory	128 GB, 8 x16 GB 2133 MT/s DDR4 RDIMM
Storage	12 x 3.5 inch 4 TB SAS 7.2 K rpm, 48 TB total, 34 TB usable (RAID 6)
Power supply	Dual redundant 750 W AC
Dimensions	29.5 inches deep x 17.7 inches wide x 2.4 inches high
Included Components	Event Collector Event Processor Flow Processor Internal storage for events and flows QRadar Data Node appliance

The QRadar 3128-C (All-in-One) requires external QRadar QFlow Collectors for layer 7 network activity monitoring.

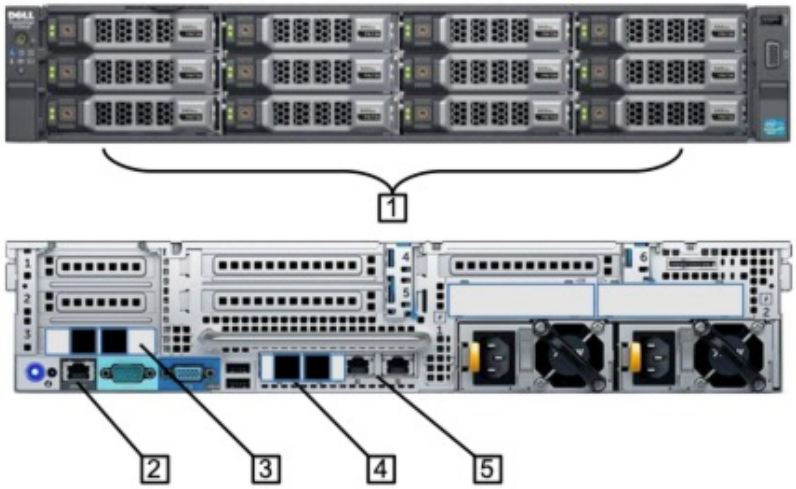


Figure 35. QRadar xx28-C

Table 70. Legend for use with the QRadar xx28-C image	
Label	**Description**
1	Event data storage
2	IMM port (1GbE TX)
3	Fibre channel ports (16 Gb TX)
4	Management ports (10 GbE SFP+)
5	Management ports (1 GbE TX)

QRadar 21xx

The IBM QRadar 2100 (MTM 4380-Q1C) appliance is an all-in-one system that combines Network Behavioral Anomaly Detection (NBAD) and Security Information and Event Management (SIEM) to accurately identify and appropriately prioritize threats that occur on your network.

Note: If you are upgrading a QRadar 21xx appliance from V7.2.8 or earlier, larger apps such as Pulse, QDI, or User Behavior Analytics can cause overall performance issues on the Console. Apps can be offloaded to a App Host to provide extra storage, memory, and CPU resources for your apps without impacting the processing capacity of your Console.

The QRadar 21xx can be used for the following appliances:

- QRadar 2100
- QRadar Log Manager 2100

View hardware information and requirements for the QRadar 21xx in the following table:

Table 71. QRadar 21xx overview	
Description	**Value**
Maximum capacity	1,000 EPS 50,000 FPM

Table 71. QRadar 21xx overview (continued)	
Description	**Value**
Interfaces	Three 10/100/1000 Base-T network monitoring interfaces One 10/100/1000 Base-T IBM QRadar management interface One 10/100/1000 Base-T integrated management module interface Two 10 Gbps SFP + ports
Memory	32 GB, 4 x 8GB 1600 MHz RDIMM
Storage	6 x 2.5 inch 500 GB 7.2K rpm SATA, 3 TB total, 1.5 TB usable (RAID 10)
Power supply	Dual Redundant 750 W AC
Dimensions	28.9 inches deep x 16.9 inches wide x 1.7 inches high
Included components	Event Collector Event Processor Single QRadar QFlow Collector

Additional QRadar QFlow Collectors are sold separately.

For more information about QRadar 21xx, including front and back panel diagrams, see IBM System X3550 M4 (https://lenovopress.com/tips0851-system-x3550-m4-e5-2600-v2).

QRadar QFlow Collector 1201

The IBM QRadar QFlow Collector 1201 (MTM 4380-Q2C) appliance provides high capacity and scalable Layer 7 application data collection for distributed deployments. The QRadar QFlow Collector 1201 also supports external flow-based data sources.

View hardware information and requirements for the QRadar QFlow Collector 1201 in the following table:

Table 72. QRadar QFlow Collector 1201	
Description	**Value**
Network traffic	1 Gbps
Interfaces	Five 10/100/1000 Base-T network monitoring interfaces Two 10 Gbps SFP + ports One 10/100/1000 Base-T QRadar management interface One 10/100/1000 Base-T integrated management module interface
Memory	16 GB, 4 x 4GB 1600 MHz RDIMM
Storage	2 x 2.5 inch 600 GB 10 K rpm SAS, 600 GB total (RAID 1)
Power supply	Dual Redundant 550 W AC
Dimensions	28.9 inches deep x 16.9 inches wide x 1.7 inches high
Included components	QRadar QFlow Collector

For more information about QRadar QFlow Collector appliances, including front and back panel diagrams, see IBM System X3550 M4 (https://lenovopress.com/tips0851-system-x3550-m4-e5-2600-v2).

QRadar QFlow Collector 1202

The IBM QRadar QFlow Collector 1202 (MTM 4380-Q3C) appliance provides high capacity and scalable Layer 7 application data collection for distributed deployments. The QRadar QFlow Collector 1202 also supports external flow-based data sources.

View hardware information and requirements for the QRadar QFlow Collector 1202 in the following table:

Table 73. QRadar QFlow Collector 1202

Description	Value
Network traffic	3 Gbps
Interfaces	Napatech Network Adapter, providing four 1 Gbps 10/100/1000 Base-T network interfaces Two 10 Gbps SFP + ports One 10/100/1000 Base-T QRadar management interface One 10/100/1000 Base-T integrated management module interface
Memory	16 GB, 4 x 4GB 1600 MHz RDIMM
Storage	2 x 2.5 inch 600 GB 10 K rpm SAS, 600 GB total (RAID 1)
Power supply	Dual Redundant 550 W AC
Dimensions	28.9 inches deep x 16.9 inches wide x 1.7 inches high
Included components	QRadar QFlow Collector NT4E-STD Napatech Network Adaptor

For more information about QRadar QFlow Collector appliances, including front and back panel diagrams, see IBM System X3550 M4 (https://lenovopress.com/tips0851-system-x3550-m4-e5-2600-v2).

QRadar QFlow Collector 1202-C/1301-C

The IBM QRadar Core Appliance QFlow Collector 1202-C and 1301-C (MTM 4380-Q1G) appliance provides high capacity and scalable Layer 7 application data collection for distributed deployments. The QRadar QFlow Collector 1202-C/1301-C also supports external flow-based data sources.

View hardware information and requirements for the QRadar QFlow Collector 1202-C/1301-C in the following table:

Table 74. QRadar QFlow Collector 1202-C/1301-C specifications

Description	Value
Network traffic	3 Gbps
Interfaces	Two 10/100/1000 Base-T network monitoring interfaces Two 10 Gbps SFP + ports One 10/100/1000 Base-T QRadar management interface One 10/100/1000 Base-T integrated management module interface Four 1 Gbps NT4E-STD SFP+ Napatech card. Supported SFP+ 1 Gbps Copper, 1 Gbps Short Range Fiber, 1 Gbps Long Range Fiber
Memory	16 GB, 4 x 4GB 1600 MHz RDIMM
Storage	600 GB 10 K rpm SAS, 600 GB total (RAID 1)

Table 74. QRadar QFlow Collector 1202-C/1301-C specifications (continued)	
Description	**Value**
Power supply	Dual Redundant 750 W AC
Dimensions	27.57 inches deep x 18.99 inches wide x 1.68 inches high
Included components	QRadar QFlow Collector

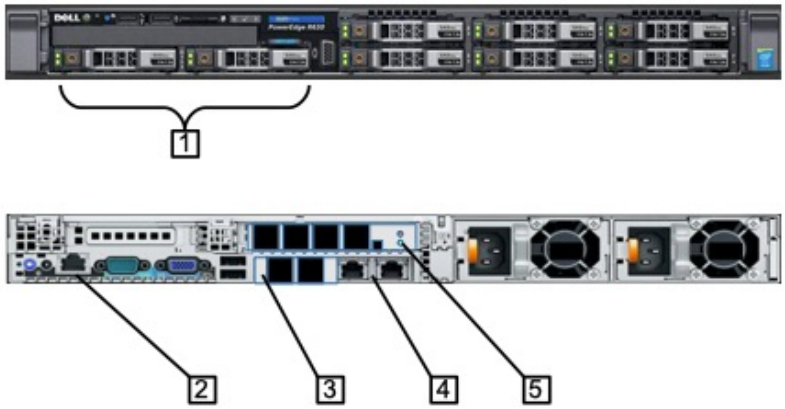


Figure 36. QRadar QFlow Collector 1202-C/1301-C

Table 75. Legend for use with the QRadar QFlow Collector 1202-C/1301-C image	
Label	**Description**
1	QRadar firmware storage
2	IMM port (1 GbE TX)
3	Management ports (10 GbE SFP+)
4	Management ports (1 GbE TX)
5	Network packet capture (SFP)

For information about battery replacement, watch the PowerEdge R630: Remove/Install System Battery video (http://www.dell.com/support/contents/us/en/19/videos/videoPlayer/R3dGJkcDrKfQHglE-qqPpuGprIpm_uF-).

QRadar QFlow Collector 1301

The IBM QRadar QFlow Collector 1301 (MTM 4380-Q4C) appliance provides high capacity and scalable Layer 7 application data collection for distributed deployments. The QRadar QFlow Collector 1301 also supports external flow-based data sources.

View hardware information and requirements for the QRadar QFlow Collector 1301 in the following table:

Table 76. QRadar QFlow Collector 1301	
Description	**Value**
Network traffic	3 Gbps

Table 76. QRadar QFlow Collector 1301 (continued)	
Description	**Value**
Interfaces	Napatech Network Adapter, providing four 1 Gbps 1000 Base SX Multi-Mode Fiber network monitoring interfaces Two 10 Gbps SFP + ports One 10/100/1000 Base-T QRadar management interface One 10/100/1000 Base-T integrated management module interface
Memory	16 GB, 4 x 4GB 1600 MHz RDIMM
Storage	2 x 2.5 inch 600 GB 10 K rpm SAS, 600 GB total (RAID 1)
Power supply	Dual Redundant 550 W AC
Dimensions	28.9 inches deep x 16.9 inches wide x 1.7 inches high
Included components	QRadar QFlow Collector NT4E-STD Napatech Network Adaptor

For more information about QRadar QFlow Collector appliances, including front and back panel diagrams, see IBM System X3550 M4 (https://lenovopress.com/tips0851-system-x3550-m4-e5-2600-v2).

QRadar QFlow Collector 1310

The IBM QRadar QFlow Collector 1310 (MTM 4380-Q5C) appliance provides high capacity and scalable Layer 7 application data collection for distributed deployments. The QRadar QFlow Collector 1310 also supports external flow-based data sources.

View hardware information and requirements for the QRadar QFlow Collector 1310 in the following table:

Table 77. QRadar QFlow Collector 1310	
Description	**Value**
Network traffic	10 Gbps
Interfaces	Napatech Network Adapter for fiber, providing two 10 Gbps SFP + network monitoring interfaces One 10/100/1000 Base-T QRadar management interface One 10/100/1000 Base-T integrated management module interface
Memory	16 GB, 4 x 4GB 1600 MHz RDIMM
Storage	2 x 2.5 inch 600 GB 10 K rpm SAS, 600 GB total (RAID 1)
Power supply	Dual Redundant 550 W AC
Dimensions	28.9 inches deep x 16.9 inches wide x 1.7 inches high
Included components	QRadar QFlow Collector NT20E2 Napatech Network Adaptor

For more information about QRadar QFlow Collector appliances, including front and back panel diagrams, see IBM System X3550 M4 (https://lenovopress.com/tips0851-system-x3550-m4-e5-2600-v2).

QRadar QFlow Collector 1310 SR-C/LR-C

The IBM QRadar Core Appliance QFlow Collector 1310SR-C and LR-C (MTM 4380-Q2G) appliance provides high capacity and scalable Layer 7 application data collection for distributed deployments. The SR model includes short range transceivers. The LR model includes long range transceivers.

View hardware information and requirements for the QRadar QFlow Collector 1310 SR-C/LR-C in the following table:

Table 78. QRadar QFlow Collector 1310 SR-C/LR-C specifications

Description	Value
Network traffic	10 Gbps
Interfaces	Two 10/100/1000 Base-T network monitoring interfaces Two 10 Gbps SFP + ports One 10/100/1000 Base-T QRadar management interface One 10/100/1000 Base-T integrated management module interface Napatech Network Adapter for fiber, providing two 10 Gbps SFP + network monitoring interfaces.
Memory	16 GB, 4 x 4GB 1600 MHz RDIMM
Storage	600 GB 10 K rpm SAS, 600 GB total (RAID 1)
Power supply	Dual Redundant 750 W AC
Dimensions	27.57 inches deep x 18.99 inches wide x 1.68 inches high
Included components	QRadar QFlow Collector NT20E2 Napatech Network Adaptor

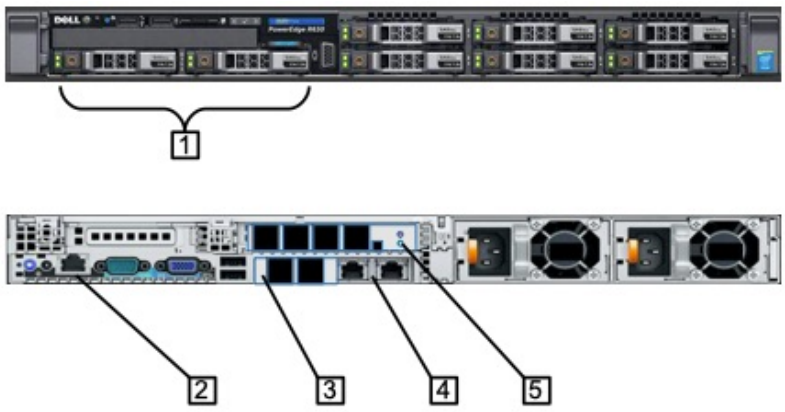


Figure 37. QRadar QFlow Collector 1310 SR-C/LR-C

Table 79. Legend for use with the QRadar QFlow Collector 1310 SR-C/LR-C image

Label	Description
1	QRadar firmware storage
2	IMM port (1 GbE TX)
3	Management ports (10 GbE SFP+)

Table 79. Legend for use with the QRadar QFlow Collector 1310 SR-C/LR-C image (continued)	
Label	**Description**
4	Management ports (1 GbE TX)
5	Network packet capture (SFP/SFP+)

For information about battery replacement, watch the PowerEdge R630: Remove/Install System Battery video (http://www.dell.com/support/contents/us/en/19/videos/videoPlayer/R3dGJkcDrKfQHglE-qqPpuGprIpm_uF-).

QRadar Event Collector 1501

The IBM QRadar Event Collector 1501 (MTM 4380-Q2C) appliance is a dedicated event collector. By default, a dedicated event collector collects and parses event from various log sources and continuously forwards these events to an event processor. You can configure the QRadar Event Collector 1501 appliance to temporarily store events and only forward the stored events on a schedule. A dedicated event collector does not process events and it does not include an on-board event processor.

View hardware information and requirements for the QRadar Event Collector 1501 in the following table:

Table 80. QRadar Event Collector 1501 specifications	
Description	**Value**
Events per second	15,000 EPS
Network traffic	1 Gbps
Interfaces	Five 10/100/1000 Base-T network monitoring interfaces Two 10 Gbps SFP + ports One 10/100/1000 Base-T QRadar management interface One 10/100/1000 Base-T integrated management module interface
Memory	16 GB, 4 x 4GB 1600 MHz RDIMM
Storage	2 x 2.5 inch 600 GB 10 K rpm SAS, 600 GB total (RAID 1)
Power supply	Dual Redundant 550 W AC
Dimensions	28.9 inches deep x 16.9 inches wide x 1.7 inches high
Included components	Event Collector

For more information about QRadar Event Collectors, including front and back panel diagrams, see IBM System X3550 M4 (https://lenovopress.com/tips0851-system-x3550-m4-e5-2600-v2).

QRadar Network Insights 1920-C

The IBM QRadar Network Insights 1920-C (MTM 4531-F3F) appliance provides detailed analysis of network flows to extend the threat detection capabilities of IBM QRadar.

The appliance has two Napatech cards, each with four ports. By default, the four ports on the first network capture card are configured for inbound traffic from the network tap. If the appliance is included in a stack, the ports are reconfigured for 2 inbound and 2 outbound. For more information about cabling stacked appliances, see the IBM QRadar Network Insights *Installation and Configuration Guide*.

The second Napatech card is cabled internally for load balancing and cannot not be used. If you use these ports when you cable the appliance, you do not get any data.

The following table shows the hardware information and requirements for the IBM QRadar Network Insights 1920-C (MTM 4531-F3F) appliance:

Table 81. QRadar Network Insights 1920-C overview

Description	**Value**
Dimensions	26.92 inches deep x 17.49 inches wide x 3.44 inches high
Power	Dual redundant 750 Watt AC power supply
Storage	2x 200 GB SSD (Raid 1) The storage is labeled as [1] in the appliance diagram.
Memory	128 GB (8 x16 GB DDR4 2400MHz)
Network capture transceivers	2x 10Gb Short Range Fiber Transceivers (Avago AFBR-703SDZ or AFBR-709SMZ) 2x 1G TX RJ-45 Transceivers (Avago ABCU-5710RZ or ABCU-5740RZ) 2x 1G SX LC Transceivers (Avago AFBR-5715PZ) Use these transceivers with the network packet capture card, labeled as [2] in the appliance diagram.
Network management transceivers	2x 10G Short Range SFP The transceivers may have one of the following part numbers: • Avago AFBR-709SMZ-IB8 • Finisar FTLX8571D3BCL-BN • BNT BN-CKM-SP-SR Use these transceivers with the management ports, labeled as [4] in the appliance diagram.

System performance of QRadar Network Insights appliances varies depending on the exact configuration and tuning of the system components. It is influenced not only by hardware, but also factors such as the search, extraction criteria, and the amount of network data. For more information, see Performance impacts in the IBM QRadar Network Insights *Installation and Configuration Guide*.

QRadar Network Insights 1920-C appliance

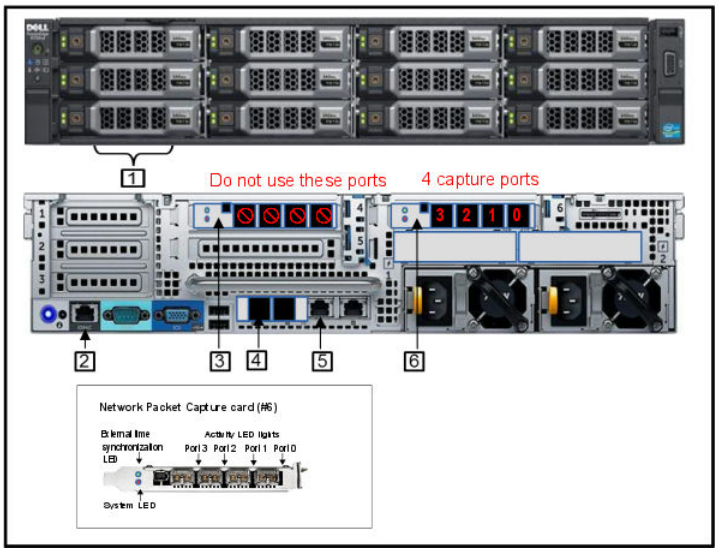


Figure 38. Back panel of the QRadar Network Insights 1920-C appliance

Table 82. Legend for use with the QRadar Network Insights 1920-C image	
Label	**Description**
1	QRadar Firmware Storage
2	IMM Port (1GbE TX)
3	Cabled internally. Do not use these ports.
4	Management ports (10 GbE SFP+)
5	Management ports (1 GbE TX)
6	Network Packet Capture (SFP/SFP+)

QRadar Incident Forensics

Use IBM QRadar Incident Forensics to retrace the step-by-step actions of a potential attacker, and conduct an in-depth forensics investigation of suspected malicious network security incidents. QRadar Incident Forensics reduces the time it takes security teams to investigate offense records. It can also help you remediate a network security breach and prevent it from happening again.

View hardware information and requirements for the QRadar Incident Forensics in the following table:

Table 83. QRadar Incident Forensics	
Description	**Value**
Interfaces	One 2-port Emulex 8Gbps FC Two 10/100/1000 Base-T network monitoring interfaces One 10/100/1000 Base-T QRadar management interface One 10/100/1000 Base-T integrated management module interface Two 10 Gbps SFP + ports
Memory	128 GB, 8 x 16 GB 1866 MHz RDIMM8
Storage	12 x 3.5 inch 4 TB SAS 7.2 K rpm, 48 TB total, 34 TB usable (RAID 6)
Power supply	Dual Redundant 900 W AC Power Supply
Dimensions	29.5 inches deep x 17.6 inches wide x 3.4 inches high

For more information about QRadar Incident Forensics appliances, including front and back panel diagrams, see IBM System X3650 M4 BD (https://lenovopress.com/tips1102-system-x3650-m4-bd).

QRadar Network Packet Capture-C

QRadar Network Packet Capture-C (MTM 4531-F2C) offers an optional QRadar Network Packet Capture-C appliance to store and manage data that is used by QRadar Incident Forensics when no other network packet capture (PCAP) device is deployed. Any number of these appliances can be installed as a tap on a network or subnetwork to collect the raw packet data.

View hardware information and requirements for the QRadar Network Packet Capture-C in the following table.

Table 84. QRadar Network Packet Capture-C	
Description	**Value**
Interfaces	Two Napatech Network Adapter for fiber, providing four 10 GbE SFP+, 1GbE SFP SR SFP+ Transceivers SX SFP Transceivers TX SFP Transceivers Three 10/100/1000 Base-T network monitoring interfaces One 10/100/1000 Base-T QRadar management interface One 10/100/1000 Base-T integrated remote system management interface Two 10 GbE SFP+ ports
Memory	128 GB, 8 x16 GB 2133 MT/s DDR4 RDIMM
Storage	2x 1 TB 2.5" SAS (RAID 1), 12x 6 TB 3.5" SAS (RAID5)
Power supply	Dual redundant 750 W AC
Dimensions	2U, 26.92 inches deep x 17.49 inches wide x 3.44 inches high

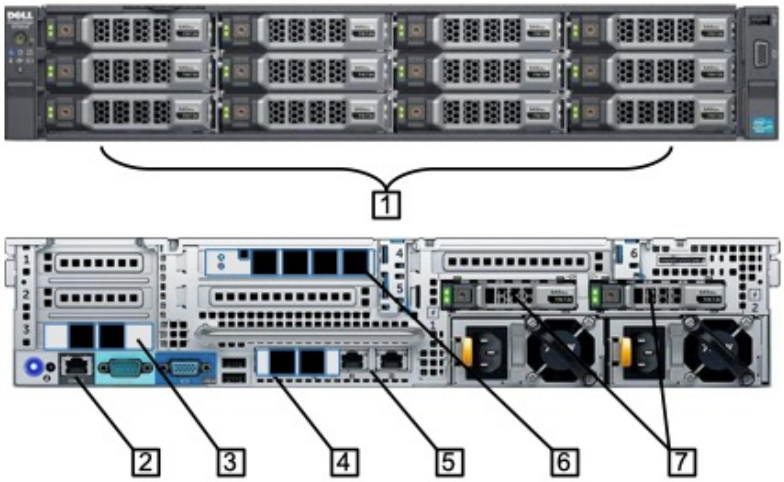


Figure 39. QRadar Network Packet Capture-C

Table 85. Legend for use with the QRadar Network Packet Capture-C image

Label	Description
1	Packet capture storage
2	IMM port (1GbE TX)
3	External RAID DAS ports
4	Management ports (10 GbE SFP+)
5	Management ports (1 GbE TX)
6	Network packet capture (SFP/SFP+)
7	QRadar firmware storage

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.

VMware, the VMware logo, VMware Cloud Foundation, VMware Cloud Foundation Service, VMware vCenter Server, and VMware vSphere are registered trademarks or trademarks of VMware, Inc. or its subsidiaries in the United States and/or other jurisdictions.

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”.

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