IBM Security QRadar Incident Forensics
V 7.3.0

QRadar Packet Capture 用户指南

备注

使用此信息及其支持的产品前，请阅读第 25 页的『声明』中的信息。

产品信息

本文档适用于 IBM QRadar Security Intelligence Platform V7.3.0 及后续发行版，直到被本文档的更新版本所取代。

目录

关于 Packet Capture 用户指南

此文档为您提供了安装和配置 IBM® QRadar® Packet Capture 所需的信息。

目标受众

复制安装 QRadar Packet Capture 的系统管理员必须了解网络安全概念和设备配置。

技术文档

要找到 QRadar 产品库中的 IBM Security QRadar 产品文档，请参阅访问 IBM Security 文档技术说明 (www.ibm.com/support/docview.wss?rs=0&uid=swg21614644)。

与客户支持人员联系

有关与客户支持人员联系的信息，请参阅支持与下载技术说明 (http://www.ibm.com/support/docview.wss?uid=swg21616144)。

有关良好安全实践的声明

IT 系统安全性涉及通过预防、检测和应对企业内外的不当访问来保护系统和信息。不当访问可能会导致信息被篡改、销毁、盗用或滥用，并可能导致系统损坏或者被滥用，包括用于攻击他人。 没有任何 IT 系统或产品应该被认为绝对安全，并且没有任何单一产品、服务或安全措施在预防不当使用或访问方面完全有效。 IBM 的系统、产品和服务设计成合法的综合性安全途径的组成部分，这必定涉及额外的操作过程，并可能需要其他系统、产品或服务才能实现最高效用。 IBM 不保证任何系统、产品或服务不受任何相关方的恶意或非法行为影响，也不保证能够使您的企业不受这些行为影响。

请注意：

使用本程序可能会涉及各种法律或法规，包括关于隐私、数据保护、雇佣以及电子通信和存储的法律或法规。IBM Security QRadar 只能用于合法目的并以合法方式使用。客户同意按照适用的法律、法规和政策使用本程序，并承担遵守适用的法律、法规和政策的所有责任。被许可方表示它将获取或已获取允许合法使用 IBM Security QRadar 所需的任何许可、许可权或许可证。

第 1 章 QRadar Packet Capture 简介

IBM Security QRadar Packet Capture 是网络流量捕获和搜索应用程序。 QRadar Packet Capture 设备仅具有一个捕获端口 (DNA0)，您可以安装 10G 或 1G SFP 收发器。

通过使用 QRadar Packet Capture，您可以高达 10 Gbps 的速度捕获来自实时网络接口的网络包，并将其写入文件，而不会出现丢包。

您可以使用 QRadar Packet Capture 按时间搜索已捕获的网络流量并将包络数据打包。通过利用充足的设备资源和经过微调的搜索，您可以同时使用搜索和记录数据，而不会出现数据丢失。

具有 10G 收发器的 QRadar Packet Capture 设备支持集群，与单个独立服务器相比，集群可扩展整体数据存储和计算能力。具有 1G 收发器的 QRadar Packet Capture 设备不支持集群。

QRadar Packet Capture 功能

QRadar Packet Capture 附带的部分功能为：

标准的 PCAP 文件格式

用于存储网络流量的文件格式。 该文件格式与现有的第三方分析工具集成。

高性能的包到磁盘记录

捕获来自活动网络的网络包。

多核支持

QRadar Packet Capture 设计用于与多核体系结构配合使用。

直接 I/O 磁盘访问

QRadar Packet Capture 使用对磁盘的直接 IO 访问权来获取最大磁盘写吞吐量。

实时建立索引

QRadar Packet Capture 可以在包捕获期间自动生成索引。 可以使用像 Berkeley 包捕获 (BPF) 一样的语法和/或 HTTP 域或基本 URL 字符串来查询该索引以在指定的时间间隔内快速检索有趣的包。

能够增加捕获数据容量的集群（仅限 10G 版本）。

您可以启用数据节点以创建集群，用于增加的存储容量。

转储格式

使用微秒分辨率时间戳记以标准 PCAP 格式保存捕获文件。捕获文件按照文件大小的顺序存储。 捕获文件存储在目录中。 根据预配置的记录参数，当目录中的空间全部占用后，将覆盖捕获文件。

捕获速度

对于包捕获设备，捕获网络流量的速度取决于是否已将数据节点连接到主节点：

- 对于未连接数据节点的包捕获设备，最大捕获速度可高达 7 Gbps。
- 对于数据节点连接到主节点的包捕获设备，捕获速度可高达 10 Gbps。

有关将包转发到 QRadar Packet Capture 的更多信息，请参阅《*IBM Security QRadar* 管理指南》。

相关概念:

第 7 页的第 3 章, 『Capture 用法概述』

要捕获磁盘流量，请启动捕获应用程序。 记录器组件将网络流量数据保存到预配置的目录中。当目录中的空间全部占用后，将覆盖现有文件。

第 2 章 QRadar Packet Capture 设置

在使用 IBM Security QRadar Packet Capture 前，需要一些基本的基本配置。

支持 Web 浏览器

支持以下 Web 浏览器：

- Google Chrome V44.0.2403.157 或更高版本。
- Mozilla Firefox V40.0.3 或更高版本。

设置网络

要使 QRadar Packet Capture 远程可用，必须为某个以太网端口（通常为 eth2、eth3 或 eth4）分配 IP 地址。 缺省情况下，将系统配置为使用 DHCP。 对于初始配置，您可能需要连接兼容 VGA 的显示器。

对于初始配置，请执行以下步骤：

1. 打开 QRadar Packet Capture 装置。
2. 使用 SSH 和端口 4477 以 root 用户身份登录。

   缺省用户名为：root。缺省密码为：P@ck3t08..

   要更改缺省密码，请参阅第 5 页的『更改操作系统帐户密码』。
3. 要确保系统是最新的，请应用 IBM Fix Central (www.ibm.com/support/fixcentral/) 上的可用软件修订。
4. 为您自己的网络配置静态 IP 地址：
   a. 要到达 MAC 地址或 eth2 接口，请输入以下命令：

      ```
      ifconfig | grep eth2
      ```

      eth0 和 eth1 接口不可用。 请将 eth2 用于 M4 xSeries 硬件。
   b. 记录 MAC 地址。
   c. 编辑 /etc/sysconfig/network-scripts/ifcfg-eth2 文件中的设置：
      - 添加以下文本作为第一行：DEVICE=eth2
      - 取消注释 eth2 端口的 MAC 地址：HWADDR=xx:xx:xx:xx:xx
      - 确保已配置以下设置：BOOTPROTO=static
      - 确保使用与网络有关的信息并且输出与以下静态示例相似：

        ```
        DEVICE=eth2
        #HWADDR=xx:xx:xx:xx:xx
        BOOTPROTO="static"
        BROADCAST="192.168.1.255"
        DNS1="0.0.0.0"
        DNS2="0.0.0.0"
        GATEWAY="192.168.1.2"
        IPADDR="192.168.1.1"
        NETMASK="255.255.255.0"
        NM_CONTROLLED="no"
        ONBOOT="yes"
        ```

5. 保存文件。
6. 要应用这些设置，请运行以下命令：

   ```
   service network restart
   ```

7. 运行以下命令来验证接口设置：

   ```
   ifconfig | more
   ```

DHCP 示例：在 CentOS6.2 中，在 /etc/sysconfig/network-scripts/ifcfg-eth0 文件或 /etc/sysconfig/network-scripts/ifcfg-eth1 文件中编辑以下设置。

```
BOOTPROTO="dhcp"
NM_CONTROLLED="no"
ONBOOT="yes"
```

远程登录

在本地设置 IP 地址后，您可以在端口 4477 上使用 SSH 进行远程登录来管理设备。

配置许可证

在使用 QRadar Packet Capture 之前，必须针对 QRadar Packet Capture 设备和 QRadar Packet Capture 软件配置许可证。

过程

1. 要针对安装了 SFP 1G 收发器的 QRadar Packet Capture 设备配置许可，请完成以下步骤：
   a. 请与您的 IBM 代表联系以获取主节点的许可证密钥。
   b. 在 QRadar Packet Capture 中，单击**帮助** > **更新主许可证**。
   c. 要将许可证应用于 QRadar Packet Capture 设备，请将值粘贴到**许可证密钥**字段。
   d. 将**系统标识**和**许可证密钥**的值粘贴到各自的字段。
   e. 单击**更新主许可证**以应用更改。
2. 要针对安装了 SFP+ 10G 收发器的 QRadar Packet Capture 设备配置许可，请完成以下步骤：
   a. 请与您的 IBM 代表联系以获取数据节点的许可证密钥。
   b. 在 QRadar Packet Capture 中，要应用主许可证，请单击**帮助** > **更新主许可证**。
   c. 将**许可证密钥**和**系统标识**的值粘贴到各自的字段。
   d. 单击**更新主许可证**以应用更改。
   e. 根据在集群中数据节点的数量，您需要通过单击**帮助** > **Node1** 进行更新。
   f. 要更新数据节点许可证，请将**许可证密钥**和**系统标识**的值粘贴到各自的字段。
   g. 要更新数据节点，请单击**更新 Node1 许可证**以应用更改。

管理用户

要使用户能够访问和使用 IBM Security QRadar Packet Capture，您必须添加用户，为其分配合适的角色，以及配置登录凭证。

开始之前

确保以 root 用户身份登录 QRadar Packet Capture。或者，确保您可以使用 sudo 命令来创建用户。

过程

1. 要创建用户，请运行以下命令：

   ```
   ./usr/local/nc/bin/nc_user_manager add <username> <password> <Admin|Guest>
   ```

   如果已存在用户名 *<username>*，那么此命令失败。

   如果指定的角色既不是管理员，也不是访客，那么此命令失败。

   添加用户后，您可以将相同的用户名和密码用于产品登录和 REST API 登录。
2. 要删除用户，请运行以下命令：

   ```
   ./usr/local/nc/bin/nc_user_manager delete <username> <password>
   ```

   如果已存在用户名 *<username>*，那么此命令失败。

   如果 *<username>* 和 *<password>* 与 QRadar Packet Capture 中记录的内容不匹配，那么此命令失败。

   删除用户后，您可以将相同的用户名和密码用于产品登录和 REST API 登录。

更改操作系统帐户密码

在设置设备后，更改 IBM Security QRadar Packet Capture 的缺省操作系统密码。

您必须是 root 用户才能更改操作系统帐户。

QRadar Packet Capture 应用程序密码与操作系统密码无关。

过程

1. 使用 SSH 以 root 用户身份登录。

   root 用户的缺省密码为 P@ck3t08..
2. 要更改 root 用户帐户的密码，请使用 **passwd** *username* 命令。

使 QRadar Packet Capture 服务器时间与 QRadar Console 系统时间同步

要确保 IBM Security QRadar 部署具有一致的时间设置以使搜索和与数据有关的功能可以正常运行，所有设备必须与 QRadar Console 设备同步。管理员必须更新 QRadar Console 设备上的 iptables，然后将其配置为接受端口 37 上的 rdate 通信。

开始之前

必须知道 QRadar Console 的 IP 地址或主机名。 该主机名必须使用 nslookup 进行正确解析。

缺省情况下，将 QRadar Packet Capture 设备的时区设置为 UTC（全球标准时间）。

过程

1. 使用 SSH 以 root 用户身份登录 QRadar Packet Capture 设备。
2. 要关闭网络时间协议 (NTP) 服务，请输入以下命令：service ntpd stop。
3. 要关闭 NTP 的检查配置，请输入以下命令：chkconfig ntpd off。
4. 通过编辑 crontab（可定时）文件，将同步调度为定时作业。
   a. 输入以下命令：crontab -e。
   b. 要将该设备配置为每隔 10 分钟与 QRadar Console 同步一次，请输入以下命令：*/10 * * * * rdate -s *Console_IP_Address*。

      将 IP 地址或主机名用于 *Console_IP_Address* 变量。
   c. 保存配置更改。
   d. 通过输入以下命令来打开 crond：

      ```
      service crond start
      chkconfig crond on
      ```
5. 更新 QRadar Console 上的 iptables 以接受来自 QRadar Packet Capture 设备的 rdate 流量。
   a. 使用 SSH 以 root 用户身份登录 QRadar Console 设备。
   b. 编辑 /opt/qradar/conf/iptables.pre 文件。
   c. 输入以下命令：

      ```
      -A QChain -m tcp -p tcp --dport 37 -j ACCEPT --src <PCAP_IP address>
      ```

      如果您拥有多个 QRadar Packet Capture 设备，请将每个 IP 地址作为单行添加。

      示例：

      ```
      QChain -m tcp -p tcp --dport 37 -j ACCEPT --src 100.100.1.10
      QChain -m tcp -p tcp --dport 37 -j ACCEPT --src 100.100.1.11
      QChain -m tcp -p tcp --dport 37 -j ACCEPT --src 100.100.1.12
      ```
   d. 保存 iptables.pre 文件。
   e. 通过输入以下命令来更新 QRadar Console 上的 iptables：

      ```
      ./opt/qradar/bin/iptables_update.pl
      ```

相关概念:

第 7 页的第 3 章, 『Capture 用法概述』

要捕获磁盘流量，请启动捕获应用程序。 记录器组件将网络流量数据保存到预配置的目录中。当目录中的空间全部占用后，将覆盖现有文件。

第 3 章 Capture 用法概述

要捕获磁盘流量，请启动捕获应用程序。 记录器组件将网络流量数据保存到预配置的目录中。当目录中的空间全部占用后，将覆盖现有文件。

故障诊断： 如果您看到未收集任何数据，请确保存在连接流量。 要捕获流量，您必须使用 Tap 或 SPAN（镜像）端口。 使用交换机上的 SPAN 端口时，如果该交换机为 SPAN 端口分配了较低优先级，那么可能会丢弃部分包。

入门

在设置系统后，请按照以下步骤登录 IBM Security QRadar Packet Capture：

1. 打开 Web 浏览器并输入以下 URL：

   `https://PCAP_IP_Address:41390`
2. 使用以下用户帐户信息登录：

   用户名： `continuum`

   密码： `P@ck3t08..`

故障诊断：如果用户在 10 分钟期限内连续 5 次无法提供正确密码，那么将锁定此用户 30 分钟。系统管理员可手动解锁用户帐户。

缺省情况下，显示"捕获状态"页面。 您可以单击**启动捕获**或**停止捕获**来控制记录。

捕获状态

"捕获状态"页面上提供了以下信息：

- **捕获接口**
- **捕获状态**
- **启动/停止时间**
- **捕获系统的持续时间**
- **吞吐率**
- **捕获的包数**
- **捕获的字节数**
- **丢弃的包数**
- **可用存储空间**

在集群配置中，针对每个已启用的数据节点显示存储使用情况。 如果由于网络配置问题或错误连接导致无法访问 QRadar Packet Capture 数据节点，那么会显示以下消息而不是存储统计信息：从属节点已启用，但当前不可访问。

故障诊断

要查看有关配置的捕获界面的系统信息，请单击**故障诊断**。

服务器信息

要查看服务器存储器信息，请单击**服务器信息**。

网络特性描述

以图像形式查看网络吞吐量。

缺省的捕获到磁盘最大吞吐量为 10 Gbps。

捕获历史记录

查看已发生或者正在进行中的包捕获的历史记录。

内联压缩

为支持取证调查，您可以在不添加物理磁盘的情况下增加可用虚拟存储容量，将原始包内容保留更长时间。 您可以使用新的内联压缩选项来存储 QRadar Packet Capture 设备上的更多数据。

压缩量与有效内容中压缩视频内容的数量有关。例如，如果有效内容中有 5% 的压缩视频，那么压缩比率为 13:1。 压缩:存储比率是未压缩大小与已压缩大小之间的比率。

表 *1.* 内联压缩比率

已压缩的视频有效内容的百分比 (%)	压缩：存储增长率
0	17:1
5	13:1
10	6:1
20	4:1
40	2.4:1

相关概念:

第 1 页的第 1 章, 『QRadar Packet Capture 简介』
IBM Security QRadar Packet Capture 是网络流量捕获和搜索应用程序。 QRadar Packet Capture 设备仅具有一个捕获端口 (DNA0)，您可以安装 10G 或 1G SFP 收发器。

相关任务:

第 5 页的『使 QRadar Packet Capture 服务器时间与 QRadar Console 系统时间同步』
要确保 IBM Security QRadar 部署具有一致的时间设置以使搜索和与数据有关的功能可以正常运行，所有设备必须与 QRadar Console 设备同步。管理员必须更新 QRadar Console 设备上的 iptables，然后将其配置为接受端口 37 上的 rdate 通信。

第 4 章 集群

使用 QRadar Packet Capture 设备作为独立的单个服务器，或者作为服务器集群。

10G 版本支持集群，与单个独立服务器相比，集群可扩展整体数据存储容量和计算能力。集群包含一个主系统。您最多可以将两个 QRadar Packet Capture 数据节点设备连接到每个 QRadar Packet Capture 主系统。

集群选项卡显示两个数据节点及其当前状态。

缺省情况下，"数据节点"不属于集群，并且状态为已禁用。

启用数据节点

在将 IBM Security QRadar Packet Capture 数据节点物理连接到 QRadar Packet Capture 主节点后，您必须启用 QRadar Packet Capture 数据节点。启用和连接 QRadar Packet Capture 数据节点创建集群以添加存储容量和提高捕获性能。

有关连接设备的信息请，请参阅：*QRadar Packet Capture Quick Reference Guide*。

开始之前

确保捕获服务器正在运行。

过程

1. 要启用数据节点，请执行以下步骤：
   a. 在**集群**选项卡中，针对每个数据节点，选择**启用**。状态显示**已连接**。
   b. 重新启动捕获服务器。现在将启用 QRadar Packet Capture 数据节点。

   在连接了 QRadar Packet Capture 数据节点且正在运行时，它们在集群中的状态将更改为"已连接"。

   在主节点连接到数据节点后，仪表板上显示的压缩（虚拟）存储器大小将包含已连接的数据节点的存储器大小。
2. 要禁用数据节点，请执行以下步骤：
   a. 在"集群"选项卡中，对于每个数据节点，选择**禁用**。状态显示**已断开连接**。
   b. 重新启动捕获服务器。QRadar Packet Capture 数据节点现在禁用，并且不再与主节点相关联。

   断开连接的数据节点不再存储数据。

   在禁用主节点后，仪表板上的压缩（虚拟）存储大小将降低。

   如果 Data Node1 或 Data Node2 获得许可，那么许可证列将显示**永久**或**评估**，这取决于使用的许可证。

第 5 章 QRadar Packet Capture 图形

在 IBM Security QRadar Packet Capture 中，使用实时或历史图形以显示包捕获统计信息。

"实时"图形

"实时"图形跟踪有关当前包捕获的以下包捕获统计信息：

- 以 Gbps（GB/秒）为单位的吞吐量
- 每秒的包总数
- 每秒的 TCP 包数
- 每秒的 UDP 包数
- 非 UDP 流量的每秒包数
- 系统事件数
- 包压缩比率

将鼠标悬停的图形上并获取此时有关图形的统计信息。

您可以单击图形上的时间点，并自动生成搜索请求。您还可以单击显示样式图标以更改图形视图。

"历史"图形

"历史"图形提供包捕获历史记录的长期概述。历史时间线选项包括 1 小时、1 天和 1 周。

将鼠标悬停的图形上并获取此时有关图形的统计信息。

单击图形中的时间点以自动生成搜索请求。

第 6 章 在某一时间范围内搜索包用于进行诊断测试

在捕获时创建的索引数据用于生成包捕获 (pcap) 文件，此文件包含匹配指定时间范围的包和包元数据信息。

限制：这些搜索仅用于诊断目的。 需要手动清除以避免填满抽取分区。

过程

1. 单击**搜索**页面。

   缺省值已输入。
2. 选择要搜索的捕获流量的接口。

   如果具有单接口配置，那么会自动选中此接口。
3. 针对要搜索的开始时间和结束时间指定值或者更改缺省值。
4. 指定 Berkeley 包过滤器 (BPF)。

   使用 BPF 语法啦指定 BPF 过滤器。 每个表达式包含一个或多个原语。 复杂过滤表达式是使用 AND、OR 和 NOT 运算符构建的。

   以下是原语过滤器示例

   ```
   ether host 00:11:22:33:44:55
   ether src host 00:11:22:33:44:55

   ip host 192.168.0.1
   ip dst host 192.168.0.1

   ip6 host 2001:0db8:85a3:0042:0000:8a2e:0371:7334
   ip6 src host 2001:0db8:85a3:0042:0000:8a2e:0371:7334

   ip net 192.168.1.0/24
   ip src net 192.168.1

   port 80
   udp port 9000
   tcp src port 80
   ```

   以下是复杂过滤示例

   ```
   ip host 192.168.1.1 and 192.168.1.2
   ip src 192.168.1.1 and dst 192.168.1.2
   ip host 192.168.1.1 and tcp port (80 or 443)
   (ip host 192.168.1.1 or 192.168.1.2) and (port 80 or 443)
   ```
5. 指定要截取的包的数目。

   要截取的最大包数目为 10,000。 如果将此数字更改为 0，那么将截取匹配时间线和过滤器的所有包。
6. 单击**开始搜索**。
7. 在搜索页面的**操作**列中，使用**分块**选项以将搜索结果拆分为较小的数据段，因此可在整个搜索请求仍在运行时访问数据。首先指定 PCAP 文件编号，然后单击**下载 PCAP 文件**，来请求搜索。

数据段为 128MB，并且最后一个数据段可以为小于 128MB 的任意大小。

8. 要查看搜索队列的状态，请查看**搜索请求队列**。
9. 要查看所有已完成的搜索的历史记录，请查看**请求日志**。
10. 清除手动搜索以确保有足够的空间用于取证恢复流程：
    a. 以 root 用户身份登陆。

       用户名：root

       密码：P@ck3t08..

    b. 运行以下命令：

       `rm -r /extraction/<name_of_search>`

       <name_of_search> 变量是"已完成的搜索"页面上的名称列。

第 7 章 配置预捕获过滤器

在将捕获的数据写入磁盘之前，预捕获过滤器过滤网络流量。

过程

1. 创建预捕获过滤器。
   a. 单击**预捕获过滤器**菜单。
   b. 输入"过滤器名称"和"搜索过滤器"选项的设置。

      捕获过滤器采用通过合取（和/或）以及可选的前置 not 连接的原语表达式形式。

      在以下示例中，将删除以端口 80 为目标的所有流量：

      ```
      not dst port 80
      ```

      在以下示例中，仅捕获这两个主机的流量，并且将删除所有其他流量：

      ```
      host 1.2.3.4 or host 1.1.1.1
      ```
   c. 通过单击**添加**完成预捕获过滤器。 添加到列表的最后一个预捕获过滤器为活动过滤器。还会显示先前过滤器的历史记录。
2. 重新启动捕获服务器以激活新添加的过滤器。
3. 通过选择**删除**，永久删除过滤器。您必须重新启动捕获服务器。

第 8 章 配置活动触发器

在网络上行发生指定的事件时，活动触发器将向您发出警报。例如，指定 IP 地址作为搜索过滤器以在捕获包含 IP 地址的流量时发出警报。

过程

1. 创建活动触发器。
   a. 单击**活动触发器**菜单。
   b. 输入"触发器名称"和"时间范围"选项的设置。
   c. 通过单击**添加**完成活动触发器。

      限制：您最多可指定五个活动触发器。
2. 在事件发生时，复审**事件日志**中的触发器事件。单击活动触发器事件将在触发的事件围绕的指定时间参数内自动生成搜索请求。搜索时间包括事件发生前的秒数和事件发生后的秒数。
3. 通过选择**删除**，删除配置的触发器。

第 9 章 对 QRadar Packet Capture 问题进行故障诊断

故障诊断是解决问题的系统方法。 故障诊断的目标是确定未按预期工作的原因以及说明如何解决该问题。

是否安装了最新版本的 QRadar Packet Capture 软件?

总是升级到软件的最新发行版。确保在应用软件更新或者任何新安装之后立即重新启动系统，从而应用更改。在集群配置中，总是确保将主和所有数据节点系统升级至相同版本。

是否具有建议的 RAID 控制器和硬盘驱动器固件?

如果遇到与 3650 M4 RAID 控制器和硬盘驱动器上安装的固件修订版相关的可靠性或性能问题，确保具有最低固件修订版：

- 对于 3650 M4，M5200 RAID 控制器固件修订版：2015 年 5 月 27 日的 V24.7.0-0052 或更高版本。

  从 Red Hat Linux 命令行运行 .bin 文件。
- 对于 IBM Lenovo，2015 年 5 月 15 日或之后的修订版。

  从 Red Hat Linux 命令行运行 .bin 文件。

是否在 BIOS 中启用了 HyperThreading?

缺省情况下，在 BIOS 中启用超线程。运行 lscpu 命令，并复审输出以确保"每个核心的线程数等于 2"。以下是 IBM 3650-M4 命令的样本输出：

```
[root@3650M4-001 bin]# lscpu
Architecture:          x86_64
CPU op-mode(s):        32-bit, 64-bit
Byte Order:            Little Endian
CPU(s):                40
On-line CPU(s) list:   0-39
Thread(s) per core:    2
Core(s) per socket:    10
Socket(s):             2
NUMA node(s):          2
Vendor ID:             GenuineIntel
CPU family:            6
Model:                 62
Stepping:              4
CPU MHz:               2800.000
BogoMIPS:              5592.04
Virtualization:        VT-x
L1d cache:             32K
L1i cache:             32K
L2 cache:              256K
L3 cache:              25600K
NUMA node0 CPU(s):     0-9,20-29
NUMA node1 CPU(s):     10-19,30-39
```

是否已正确连接捕获端口?

IBM Security QRadar Packet Capture 设备只能在接口 0 上执行捕获。

是否已正确配置以太网网络连接?

要确保已将以太网接口分配到 IP 地址，请对已连接的接口运行 `ifconfig` 命令。

如果未配置地址，请编辑相应的 `ifcfg-eth*` 文件来配置地址。

- 在此 DHCP 示例中，在 `/etc/sysconfig/network-scripts/ifcfg-`*`eth2`* 中编辑以下设置并将 *eth2* 替换为相应的设置。

  ```
  BOOTPROTO="dhcp"
  NM_CONTROLLED="no"
  ONBOOT="yes"
  ```

- 在此静态 IP 地址示例中，在 `/etc/sysconfig/network-scripts/ifcfg-`*`eth2`* 中编辑以下设置并将 *eth2* 替换为相应的设置。

  ```
  BOOTPROTO="static"
  BROADCAST="192.168.1.255"
  DNS1="0.0.0.0"
  DNS2="0.0.0.0"
  GATEWAY="192.168.1.2"
  IPADDR="192.168.1.1"
  NETMASK="255.255.255.0"
  NM_CONTROLLED="no"
  ONBOOT="yes
  ```

更改设置后，运行 `ifconfig` 命令以配置网络接口。

是否已正确配置系统时间?

缺省情况下，将系统时间设置为全球标准时间 (UTC)，并将其配置为使用网络时间协议 (NTP) 和公共服务器以保持正确的系统时间。

是否存在系统硬件问题?

1. 确保正确生成流量并由网络接口卡 (NIC) 接收。

   查看靠近接口 0 连接右侧的指示灯。 底部指示灯必须常亮，它指示连接。 顶部指示灯必须闪烁，它指示流量活动。

2. 运行 /usr/local/nc/bin/dpdk_nic_bind.py –status 命令。

   命令结果必须与以下输出相似：

```
Network devices using DPDK-compatible driver
============================================
0000:0f:00.0 '82599ES 10-Gigabit SFI/SFP+ Network Connection' drv=igb_uio
unused=ixgbe
0000:0f:00.1 '82599ES 10-Gigabit SFI/SFP+ Network Connection' drv=igb_uio
unused=ixgbe
Network devices using kernel driver
===================================
0000:07:00.0 'I350 Gigabit Network Connection' if=eth2 drv=igb unused=igb_uio
*Active*
0000:07:00.1 'I350 Gigabit Network Connection' if=eth3 drv=igb unused=igb_uio
0000:07:00.2 'I350 Gigabit Network Connection' if=eth4 drv=igb unused=igb_uio
Other network devices
=====================
<none>
```

系统是否正在捕获流量?

要确定在启动捕获会话后系统是否正在捕获流量，请使用下列某种方法：

- 查看靠近接口 0 连接右侧的指示灯。 顶部指示灯必须闪烁，它指示流量活动。
- 在"网络特性"页面上，将看到图形输出。
- 从命令行，运行 du –h /storage0/int0 命令。

  结果与以下输出相似：

```
4.4G /storage0/int0/1_0
4.9G /storage0/int0/2_0
6.4G /storage0/int0/3_0
4.9G /storage0/int0/4_0
4.9G /storage0/int0/5_0
4.9G /storage0/int0/6_0
.
.
.
1.4T /storage0/int0/
```

  如果重复运行此命令，那么所返回的子目录数量和分配数量将增加。

是否已启用 QRadar Packet Capture 数据节点?

当 QRadar Packet Capture 数据节点已物理连接到主节点时，还必须确保在 UI 中启用此数据节点以配合主服务器运行。系统当前支持最多两个 QRadar Packet Capture 数据节点。

如果**集群**选项卡显示 QRadar Packet Capture 数据节点已连接并已启用，那么在**管理**选项卡下的**更新节点(n) 许可证**屏幕中缺少**系统标识**设置，必须确保特定 QRadar Packet Capture 数据节点安装的 QRadar Packet Capture 数据节点软件版本与主节点相同。确保满足此需求后才能更新至最新软件版本。

以 root 用户身份运行以下命令以检查 QRadar Packet Capture数据节点和主节点上安装的软件版本：

```
cat /root/version.txt
```

QRadar Packet Capture 数据节点软件版本必须与主节点上安装的软件版本相同。

如何从命令行应用 QRadar Packet Capture 数据节点许可证?

要确保您正处于 QRadar Packet Capture 数据节点中，请以 root用户身份运行以下命令：

```
cat /root/version.txt
```

要验证是否已连接到 QRadar Packet Capture 数据节点，请查找版本号末尾是否追加了一个 D，例如，7.2.7.256D。

要将许可证应用于 QRadar Packet Capture 数据节点，请以 root 用户身份运行脚本：以 root 身份运行 nc_set_license.sh。

注：

- 要使新许可证生效，必须重新启动 QRadar Packet Capture 数据节点。
- 如果在制造 QRadar Packet Capture 数据节点时已授予许可，那么无需运行此脚本。系统启动后许可证即生效。

如果应用的许可证无效，那么会显示一条错误消息：

```
Warning: LicenseKey is *NOT* valid.
```

什么是 LEEF 2.0 日志记录格式?

LEEF（日志记录扩展格式）消息按如下格式添加到 /var/log/messages 文件中：

```
<DateTime> <ServerIP> LEEF: 2.0|IBM|QRadar Packet Capture|7.2.7.256|<ID>|cat=<category> msg=<message>
```

例如，当在 IP 地址为 10.91.170.20 的系统上启动包捕获服务器时，会将以下 LEEF 消息添加到 /var/log/messages 文件中：

```
May 24 22:27:49 IP_10_91_170_20 LEEF: 2.0|IBM|QRadar Packet Capture|7.2.7.256|Started|cat=PacketCapture
```

为何创建搜索请求会返回 NoSpace 错误?

如果创建搜索时 /extraction 目录已满，那么服务器会返回 NoSpace 错误。

搜索暂停时会发生什么情况?

当 /extraction 目录超出 6.7 GB 时，搜索会暂停。这样会将一条 LEEF 消息发送到 Syslog，以指示搜索已暂停。事件日志会显示类似如下警告：

```
!WARNING: Extraction Storage Full! Search cannot proceed!!
```

要确保恢复暂停的搜索，必须删除较早的原先已完成的搜索来创建空间。要删除较早的搜索，请执行以下步骤：

1. 单击**搜索**主菜单选项。
2. 在**搜索请求日志**框中，单击**删除搜索**以删除较早的搜索。

声明

本信息是为在美国国内供应的产品和服务而编写的。

IBM 可能在所有国家或地区不提供本文档中讨论的产品、服务或功能特性。有关您当前所在区域的产品和服务的信息，请向您当地的 IBM 代表咨询。任何对 IBM 产品、程序或服务的引用并非意在明示或默示只能使用 IBM 产品、程序或服务。只要不侵犯 IBM 的知识产权，任何同等功能的产品、程序或服务，都可以代替 IBM 产品、程序或服务。但是，评估和验证任何非 IBM 产品、程序或服务的操作，由用户自行负责。

IBM 公司可能已拥有或正在申请与本文档所述内容有关的各项专利。提供本文档并不意味着授予用户使用这些专利的任何许可。 您可以用书面形式将许可查询寄往：

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 U.S.A.

有关双字节字符集 (DBCS) 信息的许可查询，请与您所在国家或地区的 IBM 知识产权部门联系，或用书面方式将查询寄往：

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"按现状"提供本出版物，不附有任何种类的（无论是明示的还是默示的）保证，包括但不限于默示的有关不侵权、适销和适用于某种特定用途的保证。 某些管辖区域在某些交易中不允许免除明示或默示的保证。 因此本条款可能不适用于您。

此信息可能包含技术上或印刷上的错误。 将对此信息进行定期的更改；这些更改将编入该出版物的新修订版中。 IBM 可以随时对本出版物中描述的产品和/或程序进行改进和/或更改，而不另行通知。

本信息中对非 IBM Web 站点的任何引用都只是为了方便起见才提供的，不以任何方式充当对那些 Web 站点的保证。那些 Web 站点中的资料不是此 IBM 产品资料的一部分，使用那些 Web 站点带来的风险将由您自行承担。

IBM 可以按它认为适当的任何方式使用或分发您所提供的任何信息而无须对您承担任何责任。

本程序的被许可方如果要了解有关程序的信息以达到如下目的：(i) 使其能够在独立创建的程序和其它程序（包括本程序）之间进行信息交换，以及 (ii) 使其能够对已经交换的信息进行相互使用，请与下列地址联系：

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

只要遵守适当的条件和条款，包括某些情形下的一定数量的付费，都可获得这方面的信息。

本资料中描述的许可程序及其所有可用的许可资料均由 IBM 依据 IBM 客户协议、IBM 国际软件许可协议或任何同等协议中的条款提供。

引用的性能数据和客户示例仅用于演示目的。实际性能结果可能根据特定配置和运行条件的不同而不同。

涉及非 IBM 产品的信息可从这些产品的供应商、其出版说明或其他可公开获得的资料中获取。IBM 没有对这些产品进行测试，也无法确认其性能的精确性、兼容性或任何其他关于非 IBM 产品的声明。有关非 IBM 产品性能的问题应当向这些产品的供应商提出。

关于 IBM 未来方向或意向的声明都可随时更改或收回，而不另行通知，它们仅仅表示了目标和意愿而已。

所有 IBM 的价格均是 IBM 当前的建议零售价，可随时更改而不另行通知。经销商的价格可与此不同。

本信息包含日常业务运作所使用的数据和报表的示例。 为了尽可能完整地说明这些示例，示例中可能会包括个人、公司、品牌和产品的名称。 所有这些名字都是虚构的，若现实生活中的人物和业务企业与此相似，纯属巧合。

商标

IBM、IBM 徽标和 ibm.com® 是 International Business Machines Corp., 在全球许多管辖区域的商标或注册商标。其他产品和服务名称可能是 IBM 或其他公司的商标。IBM 商标的最新列表可从 Web 站点 www.ibm.com/legal/copytrade.shtml 上的 "Copyright and trademark information"获取。

Microsoft、Windows、Windows NT 和 Windows 徽标是 Microsoft Corporation 在美国和/或其他国家或地区的商标。

产品文档的条款和条件

根据下列条款和条件授予对这些出版物的使用许可权。

适用性

这些条款和条件是对 IBM Web 站点的任何使用条款的补充。

个人使用

您可以为了个人使用而非商业性使用复制这些出版物，但前提是保留所有专有权声明。未经 IBM 明确许可，您不得分发、显示这些出版物或其中部分出版物，也不得制作其演绎作品。

商业使用

您只能在贵公司内部复制、分发和显示这些出版物，但前提是保留所有专有权声明。未经 IBM 的明确许可，您不得制作这些出版物的演绎作品，也不得在贵公司外部复制、分发或显示这些出版物或其部分出版物。

权利

除非本许可权中明确授予，否则不得授予对这些出版物或其中包含的任何信息、数据、软件或其他知识产权的任何许可权、许可证或权利，无论明示的还是默示的。

当 IBM 认定本出版物的使用损害了其利益时，或确定上述指示信息未被正确遵守时，IBM 保留随时撤消此处授予的许可权的权利。

只有您完全遵循所有适用的法律和法规，包括所有的美国出口法律和法规，您才可以下载、出口或再出口该信息。

IBM 对这些出版物的内容不作任何保证。这些出版物"按现状"提供，不附有任何种类的（无论是明示的还是默示的）保证，包括但不限于默示的有关适销性、不侵权和适用于某种特定用途的保证。

IBM 在线隐私声明

IBM 软件产品，包括软件即服务解决方案（"软件产品"），可使用 cookie 或其他技术收集产品使用信息、帮助改善最终用户体验、定制与最终用户的交互或用于其他用途。 在许多情况下，软件产品不收集个人可标识信息。 部分软件产品可帮助您收集个人可标识信息。 如果该软件产品使用 cookie 来收集个人可标识信息，那么有关该产品使用 cookie 的具体信息如下所述。

根据部署的配置，"软件产品" 可能使用会话 cookie 来收集每个用户的会话 ID，以用于会话管理和认证用途。 可以禁用 cookie，但是这也将删除 cookie 启用的功能。

如果为此软件产品部署的配置提供您以客户身份通过 cookie 或其他技术从最终用户收集个人可标识信息的功能，那么您应该查找关于适用于此类数据收集的所有法律的您自己的合法建议（包括声明和许可）。

有关使用各种技术（包括 cookie）来达到这些目的的更多信息，请参阅 IBM 隐私策略 (http://www.ibm.com/privacy) 和 IBM 在线隐私声明 (http://www.ibm.com/privacy/details) 中标题为"Cookies, Web Beacons and Other Technologies"的部分，以及"IBM Software Products and Software-as-a-Service Privacy Statement"(http://www.ibm.com/software/info/product-privacy)。

Printed in China