IBM Security QRadar
V 7.3.3

管理指南

备注

使用此信息及其支持的产品前，请阅读第 209 页的『声明』中的信息。

产品信息

本文档适用于 IBM® QRadar® Security Intelligence Platform V7.3.3 及后续发行版，直到被本文档的更新版本所取代。

目录

QRadar 产品管理简介

管理员使用 IBM QRadar SIEM 来管理仪表板、攻击、日志活动、网络活动、资产和报告。

目标读者

本指南旨在面向所有负责调查和管理网络安全性的 QRadar SIEM 用户。本指南假设您具有 QRadar SIEM 访问权，并具备企业网络和联网技术的知识。

技术文档

要在 Web 上查找 IBM QRadar 产品文档，包括所有翻译的文档，请访问 IBM Knowledge Center (http://www.ibm.com/support/knowledgecenter/SS42VS/welcome)。

有关如何在 QRadar 产品库中访问更多技术文档的信息，请参阅 QRadar Support - Assistance 101 (https://ibm.biz/qradarsupport)。

与客户支持人员联系

有关联系客户支持的信息，请参阅支持和下载技术说明 (http://www.ibm.com/support/docview.wss?rs=0&uid=swg21612861)。

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，并且可能需要其他系统、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:

使用本程序可能会牵涉到各种法律或法规，包括那些与隐私、数据保护、雇佣以及电子通信和存储相关的法律或法律。IBM QRadar 只能以合法方式用于合法之目的。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 QRadar 所需的任何许可、许可权或许可证。

第 1 章 针对管理员的新增内容

了解有关使您更易于配置和管理 IBM QRadar 部署的新功能部件和功能的信息。

QRadar V7.3.3 中的新功能和增强功能

下列新功能和增强功能使得管理员可以更轻松地管理其 IBM QRadar V7.3.3 部署。

要查看此发行版中所有新功能的列表，请参阅 IBM Knowledge Center (www.ibm.com/support/knowledgecenter/SS42VS_7.3.3/com.ibm.qradar.doc/c_pdf_launch.html) 上的《新增功能》文档。

在 DSM 编辑器中增强对“名称值对”事件的解析支持

在 DSM 编辑器中，现在可以从“名称值对”格式的事件轻松解析标准属性和定制属性，而无需编写正则表达式 (regex)。针对使用“名称值对”事件的日志源类型启用**属性**自动发现后，所有可用字段都将解析为定制属性。使用这些新功能，管理员和有权创建定制属性的用户都可以轻松快捷地解析这些事件。

使用 DSM 编辑器来创建定制日志源类型，以在 IBM QRadar 中处理“名称值对”事件。添加定制属性以帮助解析现有日志源类型。使用“名称值对”简单表达式而不是正则表达式来定义如何解析定制属性。DSM 编辑器根据“名称值对”规范中预定义的键，自动为系统属性提供表达式。

开启“名称值对”属性自动发现，以在针对日志源类型接收到的任何事件中，发现所有“名称值对”字段的定制属性。在**定制事件属性编辑器**中，以及手动创建日志源扩展时，也可以使用“名称值对”表达式。

下图显示在 DSM 编辑器中解析“名称值对”事件的位置。

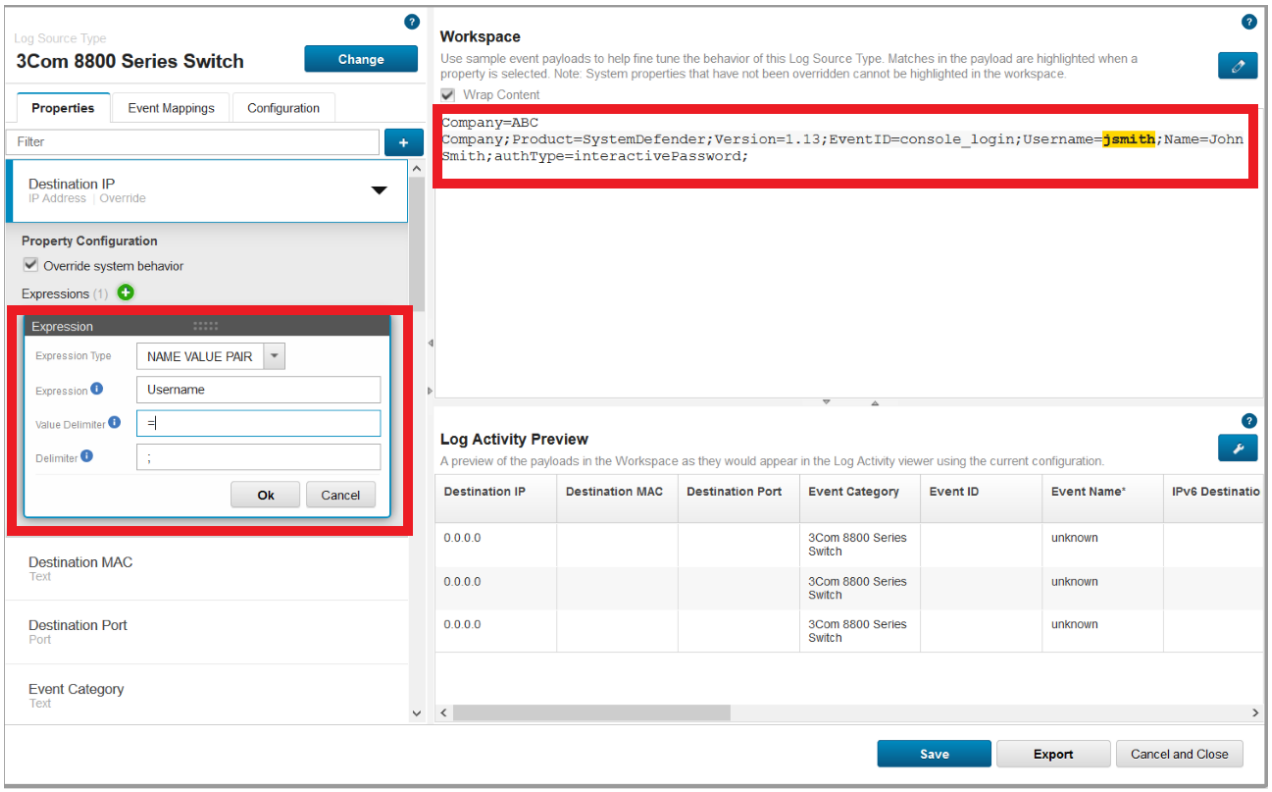

图 1. “名称值对”结构化数据类型

了解有关针对“名称值对”事件的增强解析支持的更多信息...

增强对“通用列表”事件的解析支持

在 DSM 编辑器中，现在可以从“通用列表”格式的事件轻松解析标准属性和定制属性，而无需编写正则表达式 (regex)。针对使用“通用列表”事件的日志源类型启用**属性**自动发现后，所有可用字段都将解析为定制属性。使用这些新功能，管理员和有权创建定制属性的用户都可以轻松快捷地解析这些事件。使用这些新功能，管理员和有权创建定制属性的用户都可以轻松快捷地解析这些事件。

使用 DSM 编辑器来创建定制日志源类型，以在 IBM QRadar 中处理“通用列表”事件。您还可以添加定制属性，以帮助解析 DSM 编辑器中的现有日志源类型。使用“通用列表”简单表达式而不是正则表达式来定义如何解析定制属性。DSM 编辑器根据“通用列表”规范中预定义的键，自动为系统属性提供表达式。

开启“通用列表”属性自动发现，以在针对日志源类型接收到的任何事件中，发现所有“通用列表”字段的定制属性。在**定制事件属性编辑器**中，以及手动创建日志源扩展时，也可以使用“通用列表”表达式。

下图显示在 DSM 编辑器中解析“通用列表”事件的位置。

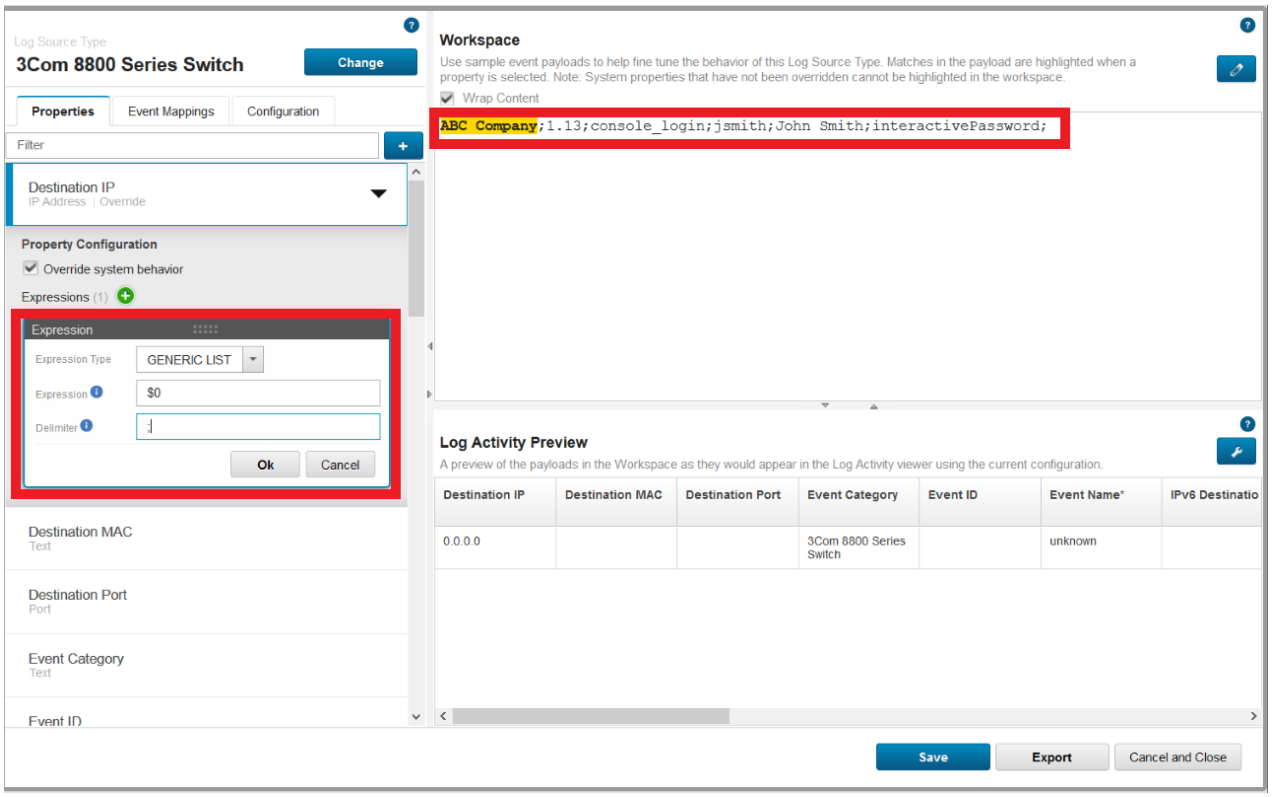

图 2. “通用列表”结构化数据类型

了解有关针对“通用列表”事件的增强解析支持的更多信息...

在卸载内容扩展时移除参考数据

在 IBM QRadar V7.3.3 中卸载内容扩展时，任何由该内容扩展安装的参考数据都会移除，或还原为其先前状态。现在在您卸载内容扩展时，参考数据被移除，这将释放系统上的磁盘空间。

以前，QRadar 移除应用程序、规则、定制属性和已保存的搜索，但是不移除参考数据，这可能会影响性能。

了解有关卸载内容扩展的更多信息...

在 DSM 编辑器中更快地导出内容

IBM QRadar V7.3.3 使在 DSM 编辑器中导出定制内容变得更快。使用**导出**按钮轻松地将您的内容从一个 QRadar 部署导出到另一个部署，或导出到外部介质。以前，您只能使用内容管理工具脚本导出定制内容。

下图显示在 DSM 编辑器中导出内容的位置。

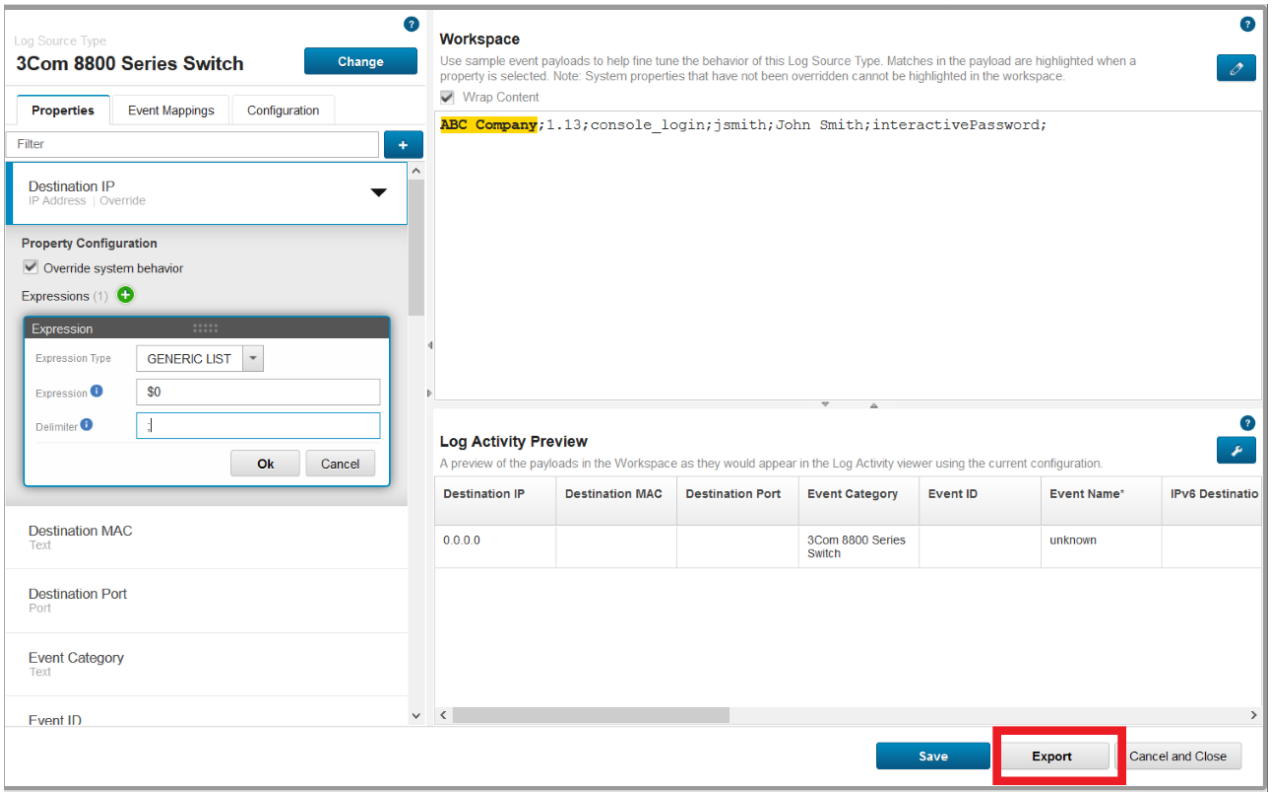

图 *3.* 从 *DSM* 编辑器导出内容

了解有关从 DSM 编辑器导出内容的更多信息...

QRadar V7.3.2 中的新功能和增强功能

下列新功能和增强功能使得管理员可以更轻松地管理其 IBM QRadar V7.3.2 部署。

要查看此发行版中所有新功能的列表，请参阅 IBM Knowledge Center (www.ibm.com/support/knowledgecenter/SS42VS_7.3.2/com.ibm.qradar.doc/c_pdf_launch.html) 上的新增内容文档。

整合式审计事件使监视变得轻松方便

缺省情况下，每个到期的参考数据元素从参考集中移除时，都会记录为单独的审计事件。大量到期元素会导致 `qradar.log` 文件变得杂乱无章。

在 QRadar V7.3.2 中，可以将同时移除的到期参考数据元素记录为一个审计事件，或选择完全不记录。审计事件较少，您可以更轻松地监视对 QRadar 进行的其他重要更改。

了解有关参考集选项的更多信息...

利用审计事件更全面地监视新攻击

创建攻击时，它会触发 QRadar 标识 (QID) 为 28250369 的审计事件，该标识可供 QRadar 搜索、过滤器和规则测试条件使用。

例如，您可以调度每日报告，以显示过去 24 小时内创建的攻击。

了解有关记录的操作的更多信息...

针对每个域或租户配置的数据模糊处理

在 QRadar V7.3.2 中，可以为每个域或租户配置模糊处理。

数据模糊处理可以阻止对存储在 QRadar 中的敏感或个人可识别信息进行未经授权的访问。

以前，模糊处理并非针对每个域或租户的日志源类型来配置。变通方法是针对各个日志源来配置模糊处理，存在许多日志源时，这种方法不切实际。

了解有关创建数据模糊处理表达式的更多信息...

使用 SAML 2.0 进行单点登录认证

IBM QRadar V7.3.2 支持安全性断言标记语言 (SAML) 2.0 单点登录格式。

通过使用 SAML 认证功能，您可以轻松地将 QRadar 与企业身份服务器集成，以提供单点登录。SAML 使您不需要为 QRadar 维护本地用户。

利用 SAML 单点登录认证，向身份服务器进行认证的用户可以自动向 QRadar 进行认证。这些用户无需记住单独的密码，也无需每次访问 QRadar 时输入凭证。

了解有关 QRadar 中的 SAML 的更多信息...

QRadar V7.3.1 中的新功能和增强功能

下列新功能和增强功能使得管理员可以更轻松地管理其 IBM QRadar V7.3.3 部署。

要查看此发行版中所有新功能的列表，请参阅 IBM Knowledge Center (www.ibm.com/support/knowledgecenter/SS42VS_7.3.1/com.ibm.qradar.doc/c_pdf_launch.html) 上的新增内容文档。

事件收集服务的停机时间已缩短

在较早版本中，将更改部署到 QRadar 系统有时会导致在 `hostcontext` 服务重新启动时数据收集出现间隔。为了最大程度地减少这些中断，现在事件收集服务已与其他 QRadar 服务分离，单独进行管理。新的事件收集服务 `ecs-ec-ingress` 侦听端口 7787。

通过这种新的服务分离，事件收集服务不会在您每次部署更改时都自动重新启动。只有在所部署的更改直接影响事件收集服务时，该服务才会重新启动。

此增强功能显著减少了收集数据时发生的中断，并使您可以更轻松地符合贵组织的数据收集目标。

了解有关在 QRadar 部署中进行更改的更多信息...

在次要补丁更新期间继续进行事件收集

对 QRadar V7.3.1 或更高版本应用将来的补丁后，事件收集的中断情况应该会有所减少。不要求系统重新启动的次要补丁不会重新启动事件收集服务。

能够仅重新启动事件收集服务

从 QRadar 产品界面中，可以在部署中的所有受管主机上重新启动事件收集服务。

当您想要重新启动事件收集服务而不影响其他 QRadar 服务时，此新功能非常有用。例如，复原配置备份之后，可以将服务重新启动延迟至您方便的时间。

了解有关重新启动事件收集服务的更多信息...

安装或更新协议 RPM 时，事件收集会继续执行

在 QRadar V7.3.1 以前，安装或更新协议 RPM 需要执行完全部署，这会造成针对所有已安装协议的事件收集停止数分钟。

现在，协议会在您部署更改时自动装入。只有已更新的协议会出现短暂的中断（数秒）。

含收藏项选项卡的新滑出式导航菜单

随着部署中安装的应用程序数量增加，可见的选项卡数量也会增加。新的滑出式导航菜单使您更便于通过管理 QRadar 中可见的选项卡来查找使用频率最高的应用程序。

升级到 QRadar V7.3.3 之后，所有的 QRadar 选项卡都可从滑出式菜单 (☰) 中访问。每个菜单项都标记为收藏项，因此也以选项卡形式提供。您可以选中或取消选中菜单项旁边的星，以控制哪些选项卡可见。

要访问旧版本 QRadar 中的**管理**选项卡上的设置，请单击滑出式导航菜单底部的**管理**。

IPv6 支持

QRadar 使用网络层次结构对象和组来查看网络中的网络活动以及监视组或服务。网络层次结构可由某个范围内的 IPv6 及 IPv4 格式的 IP 地址定义。除网络层次结构之外，Offense Manager 以前仅支持 IPv6 索引，但现在能够以 IPv6 数据更新并显示攻击的所有相应字段。

了解有关 QRadar 部署中的 IPv6 寻址的更多信息...

通过在 QRadar 中运行报告来监视成功登录事件

通过在 QRadar **报告**选项卡上运行**每周成功登录事件**报告模板，可以轻松监视您配置的时间段内的成功登录事件。

QRadar V7.3.1 中两个预先安装的新应用程序

应用程序授权管理器

应用程序授权管理器应用程序可提高应用程序授权令牌的安全性。具有适当许可权的用户可删除授权令牌或更改所分配的用户级别权限。

QRadar 助手应用程序

QRadar 助手应用程序在**仪表板**选项卡上提供以下功能：

- 建议的应用程序和内容扩展（基于所配置的首选项）。
- “QRadar 帮助中心”仪表板窗口小部件，用于帮助您访问有用的 QRadar 相关信息。
- 内容更新状态将会突出显示，用户可从 QRadar 中下载更新。
- IBM Security 支持中心 Twitter 订阅源。

配置日志源类型的自动属性发现以及 DSM 编辑器中新增的“配置”选项卡

您可以配置针对日志源类型的新属性自动发现。缺省情况下，日志源类型的“自动属性发现”选项处于禁用状态。当您在 DSM 编辑器中新增的**配置**选项卡上启用此选项时，会自动生成新属性。新属性会捕获所选日志源类型接收到的事件中存在的所有字段。新发现的属性会显示在 DSM 编辑器的**属性**选项卡中。

了解有关 DSM 编辑器中的属性配置的更多信息...。

日志源扩展可通过键引用以 JSON 格式抽取值事件

日志源扩展现在可使用 JsonKeypath 抽取值。

对于嵌套的 JSON 格式的事件数据，有效 JSON 表达式的格式为 /"<顶级字段的名称>"/"<子级字段 *1* 的名称>"*.../*"<子级字段 *n* 的名称>"。

下列两个示例说明如何从 JSON 记录中抽取数据：

- 平面 JSON 记录的简单事件情况：`{"action": "login", "user": "John Doe"}`

  要抽取“user”字段，请使用以下表达式：`/"user"`。
- 包含嵌套对象的 JSON 记录的复杂事件情况：`{ "action": "login", "user": { "first_name": "John", "last_name": "Doe" } }`

  要从“user”子对象中仅抽取“last_name”值，请使用以下表达式：`/"user"/"last_name"`。

QRadar V7.3.0 中的新功能和增强功能

IBM QRadar V7.3.0 引入面向租户用户的新功能，改善安全性，提高管理许可证时的灵活性，并且引入用于共享应用程序的专用应用程序节点。

日志源限制已移除

现在，QRadar V7.3.0 中针对许可模型的改进使您管理日志源更加轻松。日志源限制已移除，您不再需要为日志源购买许可证。

在升级到 QRadar V7.3.0 时，先前的日志源限制已移除。

租户用户可创建定制属性

租户用户可以创建定制属性，以从事件或流有效内容中抽取或计算重要信息，无需受管安全服务提供程序 (MSSP) 管理员协助。利用此功能，租户用户可以查看和搜索 QRadar 通常不会规范化并显示的数据。

作为 MSSP 管理员，您对于由租户用户创建的所有定制属性都具有写许可权。规则和报告中频繁使用租户的定制属性时，您可以优化这些属性，以改善搜索性能。租户用户不能优化他们自己创建的属性。

有关使用定制事件和流属性的信息，请参阅《*IBM QRadar User Guide*》。

租户用户可以创建参考数据集合

在 QRadar V7.2.8 中，租户用户可以查看其 MSSP 管理员所创建的参考数据。现在，在 V7.3.0 中，具有**委派管理 > 管理参考数据**用户角色的租户用户可以在没有 MSSP 管理员帮助的情况下创建并管理器自己的参考数据集合。

通过此功能，租户用户可以跟踪引用的业务数据或来自外部源的数据，这些数据随后可在 QRadar 搜索、过滤器、规则测试条件和规则响应中进行使用。例如，包含离职员工用户标识的参考集可以用于阻止此类员工登录网络。

了解有关创建和管理参考数据集合的更多信息...

安全性更新

QRadar V7.3.0 使用 TLS 1.2（传输层安全性）进行安全通信。不支持安全套接字层 (SSL) 和 TLS 1.1 协议。

当代理服务器执行自动更新时，对于用来更新缺省 CA 证书的步骤存在细微更改。

第 2 章 QRadar 管理

作为 IBM QRadar 管理员，您可以使用不同工具来帮助配置和管理 QRadar 部署。

例如，在**管理**选项卡上使用工具，可执行以下任务：

- 部署和管理 QRadar 主机和许可证。
- 配置用户帐户和认证。
- 构建网络层次结构。
- 配置域和设置多域环境。
- 定义和管理日志和流数据源。
- 管理 QRadar 数据保留时间。
- 管理资产和参考数据。
- 调度 QRadar 配置和数据的定期备份。
- 监视受管主机的系统运行状况。

IBM QRadar 产品中的功能

IBM QRadar 产品文档描述了可能仅在部分 QRadar 产品中可用的功能，例如攻击、流程、资产和历史关联。根据您所使用的产品不同，文档中记录的某些功能在您的部署中可能不可用。

IBM QRadar Log Manager

QRadar Log Manager 是基本、高性能和可伸缩的解决方案，用于收集、分析、存储和报告大量网络和安全事件日志。

IBM QRadar SIEM

QRadar SIEM 是高级产品，为本地部署提供了全套安全情报功能。它将合并来自分布于整个网络中的数千个资产、设备、端点和应用程序的日志源和网络流数据，并对原始数据执行立即的规范化和关联活动，以区分真实威胁与误报。

IBM QRadar on Cloud

QRadar on Cloud 提供 IBM 安全专家以管理基础结构，而安全分析人员则执行威胁检测和管理任务。您可以保护网络，并满足合规性监视和报告要求，同时减少所有权总成本。

QRadar 产品功能

请复审下表来比较各 QRadar 产品中的功能。

表 *1. QRadar* 功能的比较

功能	QRadar SIEM	IBM QRadar on Cloud	IBM QRadar Log Manager
完整管理功能	是	否	是
支持托管部署	否	是	否
可定制的仪表板	是	是	是
定制规则引擎	是	是	是
管理网络和安全事件	是	是	是
管理主机和应用程序日志	是	是	是
基于阈值的警报	是	是	是

表 1. *QRadar* 功能的比较 *(续)*			
功能	**QRadar SIEM**	**IBM QRadar on Cloud**	**IBM QRadar Log Manager**
合规性模板	是	是	是
数据归档	是	是	是
IBM Security X-Force® Threat Intelligence IP 声誉订阅源集成	是	是	是
WinCollect 单机部署	是	是	是
WinCollect 受管部署	是	否	是
网络活动监视	是	是	否
资产概要分析	是	是	否 [1]
攻击管理	是	是	否
网络流捕获与分析	是	是	否
历史关联	是	是	否
QRadar Network Insights 集成	是	是	否
QRadar Vulnerability Manager 集成	是	是	是
QRadar Risk Manager 集成	是	否	否
QRadar Incident Forensics 集成	是	否	否
漏洞评估扫描程序	是	是	是
[1] 只有在安装了 QRadar Vulnerability Manager 时，QRadar Log Manager 才会跟踪资产数据。			

某些文档（例如，管理指南和用户指南）在多个产品中很常见，并可能描述了部署中不可用的功能。例如，IBM QRadar on Cloud 用户不具有如 《*IBM QRadar* 管理指南》 中所描述的完整的管理功能。

支持 Web 浏览器

为了使 IBM QRadar 产品中的功能正常工作，必须使用支持的 Web 浏览器。

下表列出支持的 Web 浏览器版本。

表 2. *QRadar* 产品支持的 *Web* 浏览器	
Web 浏览器	**支持的版本**
64 位 Mozilla Firefox	60 扩展支持发行版和更高版本
64 位 Microsoft Edge	38.14393 和更高版本
Microsoft Internet Explorer	11.0
64 位 Google Chrome	最新

安全性例外和证书

如果要使用 Mozilla Firefox Web 浏览器，您必须向 Mozilla Firefox 添加例外，才能登录 QRadar SIEM。有关更多信息，请参阅您的 Mozilla Firefox Web 浏览器文档。

如果要使用 Microsoft Internet Explorer Web 浏览器，那么在您访问 QRadar SIEM 系统时显示 Web 站点安全证书消息。您必须选择**继续到此 Web 站点选项**，才能登录 QRadar SIEM。

在基于 Web 的应用程序中导航

当您使用 QRadar SIEM 时，请使用 QRadar SIEM 用户界面中可用的导航选项，而不是 Web 浏览器**返回**按钮。

第 3 章 用户管理

您可以定义用户角色、安全概要文件和用户帐户来控制谁有权访问 IBM QRadar，他们可以执行哪些任务及其有权访问哪些数据。

初始配置 QRadar 时，请使用**管理**选项卡上的**用户管理**功能部件来配置和管理所有需要 QRadar 访问权的用户的用户帐户。

相关概念

IBM QRadar 产品中的功能

安全概要文件

安全概要文件定义用户可访问的网络、日志源和域。

QRadar 包含一个用于管理用户的缺省安全概要文件。**管理员**安全概要文件包含对所有网络、日志源和域的访问权。

在添加用户帐户之前，必须创建更多安全概要文件以满足用户的特定访问需求。

域

必须使用关联的域更新安全概要文件。您必须先在“**域管理**”窗口上定义域，然后**域**选项卡才会显示在“**安全概要文件管理**”窗口上。在更新安全概要文件以及部署更改前，不会应用域级别限制。

域分配优先于**许可权优先顺序**、**网络**和**日志源**选项卡上的所有设置。

如果将域分配给租户，那么租户名称在“**已分配的域**”窗口中域名旁边的方括号内显示。

许可权优先顺序

许可权优先顺序确定系统在**日志活动**选项卡中显示事件并在**网络活动**选项卡中显示流时考虑的安全概要文件的组件。

在创建安全概要文件时选择以下限制：

- **无限制** - 此选项不对**日志活动**选项卡中显示的事件以及在**网络活动**选项卡中显示的流施加限制。
- **仅网络** - 此选项限制用户只能查看与此安全概要文件中指定的网络相关的事件和流。
- **仅日志源** - 此选项限制用户只能查看与此安全概要文件中指定的日志源相关的事件。
- **网络和日志源** - 此选项允许用户仅查看与此安全概要文件中指定的日志源和网络相关的事件和流。

  例如，如果安全概要文件允许从日志源访问事件，但是限制目标网络，那么不会在**日志活动**选项卡中显示事件。事件必须匹配两个需求。
- **网络或日志源** - 此选项允许用户查看与此安全概要文件中指定的日志源或网络相关的事件和流。

例如，如果安全概要文件允许访问来自日志源的事件，但目标网络受限，那么如果许可权优先顺序设置为**网络 OR 日志源**，事件会显示在**日志活动**选项卡上。如果许可权优先顺序设置为**网络 AND 日志源**，那么事件不会显示在**日志活动**选项卡上。

攻击数据的许可权优先顺序

在显示攻击数据时，安全概要文件自动使用**网络或日志源**许可权。例如，如果攻击具有一个安全概要文件允许使用的目标 IP 地址，但是安全概要文件未授予源 IP 地址许可权，那么“**攻击摘要**”窗口同时显示目标和源 IP 地址。

创建安全概要文件

要添加用户帐户，必须首先创建满足用户特定访问需求的安全概要文件。

关于此任务

IBM QRadar SIEM 包含一个管理用户的缺省安全概要文件。“管理”安全概要文件包含对所有网络、日志源和域的访问权。

要在“**安全概要文件管理**”窗口上选择多个项，请按住 Control 键，同时选择要添加的每个网络或网络组。

如果要在保存配置之前移除一个或多个添加的网络、日志源或域，那么可选择项，并单击**移除 (<)** 图标。要移除所有项，请单击**全部移除**。

过程

1. 在导航菜单（☰）上，单击**管理**。
2. 单击**系统配置 > 用户管理**。
3. 单击**安全概要文件**图标。
4. 在“**安全概要文件管理**”窗口工具栏上，单击**新建**。
5. 配置以下参数：
   a) 在**安全概要文件名称**字段中，输入安全概要文件的唯一名称。安全概要文件名称必须满足以下需求：最少 3 个字符，最多 30 个字符。
   b) 可选：输入安全概要文件的描述。最大字符数为 255。
6. 单击**许可权优先级**选项卡。
7. 在“许可权优先级设置”窗格中，选择许可权优先级选项。请参阅第 11 页的『许可权优先顺序』。
8. 配置要分配给安全概要文件的网络：
   a) 单击**网络**选项卡。
   b) 从**网络**选项卡左侧窗格的导航树中，选择希望此安全概要文件可访问的网络。
   c) 单击**添加 (>)** 图标以将网络添加到“分配的网络”窗格。
   d) 针对要添加的每个网络重复以上操作。
9. 配置要分配给安全概要文件的日志源：
   a) 单击**日志源**选项卡。
   b) 从左侧窗格的导航树中，选择希望此安全概要文件可访问的日志源组或日志源。
   c) 单击**添加 (>)** 图标以将日志源添加到“分配的日志源”窗格。
   d) 针对要添加的每个日志源重复以上操作。
10. 配置要分配给安全概要文件的域：
    a) 单击**域**选项卡。
    b) 从左侧窗格的导航树中，选择希望此安全概要文件可访问的域。
    c) 单击**添加 (>)** 图标以将域添加到“分配的域”窗格。
    d) 针对要添加的每个域重复以上操作。
11. 单击**保存**。

    注: 分配到安全概要文件的日志源和域必须匹配。如果日志源和域不匹配，那么无法保存安全概要文件。
12. 关闭“**安全概要文件管理**”窗口。
13. 在**管理**选项卡上，单击**部署更改**。

编辑安全概要文件

您可以编辑现有安全概要文件，以更新用户可访问哪些网络和日志源以及许可权优先级。

关于此任务

要在“**安全概要文件管理**”窗口上快速找到要编辑的安全概要文件，可以在**输入以过滤**文本框中输入安全概要文件名称。它位于左侧窗格上方。

过程

1. 在导航菜单（☰）上，单击**管理**。
2. 单击**系统配置 > 用户管理**。
3. 单击**安全概要文件**图标。
4. 在左侧窗格中，选择要编辑的安全概要文件。
5. 在工具栏上，单击**编辑**。
6. 根据需要更新参数。
7. 单击**保存**。
8. 如果“**安全概要文件具有时间序列数据**”窗口打开，请选择以下其中一个选项：

选项	描述
保留旧数据并保存	选择此选项以保存先前累积的时间序列数据。如果选择此选项，那么具有此安全概要文件的用户在查看时间序列图表时，可能会看到其无权查看的先前数据。
隐藏旧数据并保存	选择此选项以隐藏时间序列数据。如果选择此选项，那么在部署配置更改后，会重新启动时间序列数据累积。

9. 关闭“**安全概要文件管理**”窗口。
10. 在**管理**选项卡上，单击**部署更改**。

复制安全概要文件

如果要创建的新安全概要文件与现有安全概要文件匹配程度很高，那么可复制现有安全概要文件，然后修改参数。

关于此任务

要在“安全概要文件管理”窗口上快速找到要复制的安全概要文件，可以在左侧窗格上方的**输入以过滤**文本框中输入安全概要文件名称。

过程

1. 在导航菜单（☰）上，单击**管理**。
2. 单击**系统配置 > 用户管理**。
3. 单击**安全概要文件**。
4. 在左侧窗格中，选择要复制的安全概要文件。
5. 在工具栏上，单击**复制**。
6. 在“**确认**”窗口中，输入复制的安全概要文件的唯一名称。
7. 单击**确定**。
8. 根据需要更新参数。
9. 关闭“**安全概要文件管理**”窗口。
10. 在**管理**选项卡上，单击**部署更改**。

删除安全概要文件

如果不再需要安全概要文件，那么可以删除安全概要文件。

关于此任务

如果向要删除的安全概要文件分配了用户帐户，那么必须将这些用户帐户重新分配给其他安全概要文件。IBM QRadar SIEM 会自动检测此情况，并提示您更新用户帐户。

要在“**安全概要文件管理**”窗口上快速找到要删除的安全概要文件，可以在**输入以过滤**文本框中输入安全概要文件名称。它位于左侧窗格上方。

过程

1. 在导航菜单（☰）上，单击**管理**。
2. 单击**系统配置 > 用户管理**。
3. 单击**安全概要文件**。
4. 在左侧窗格中，选择要删除的安全概要文件。
5. 在工具栏上，单击**删除**。
6. 单击**确定**。
7. 将列出的用户帐户重新分配给另一个安全概要文件：
   a) 从**要分配的用户安全概要文件**列表框中，选择安全概要文件。
   b) 单击**确认**。
8. 关闭“**安全概要文件管理**”窗口。
9. 在**管理**选项卡上，单击**部署更改**。

用户帐户

用户帐户定义用于登录到 IBM QRadar 的唯一用户名，并指定将用户分配到哪个用户角色、安全概要文件和租户分配。

初始配置系统时，您必须为需要 QRadar 访问权的每个用户创建用户帐户。

查看和编辑当前用户的相关信息

您可使用主要产品界面来查看和编辑当前用户的帐户信息。

过程

1. 在主要产品界面的右上角，单击用户图标。
2. 单击**用户首选项**。
3. 更新可配置用户详细信息。

参数	描述
电子邮件	输入要与此用户关联的电子邮件地址。地址不能包含超过 255 个字符，而且不能包含空格。
当前密码	输入当前密码。
新密码	输入使用户能够获取访问权的新密码。密码必须满足密码策略强制实施的最小长度和复杂性需求。
确认新密码	再次输入新密码。
语言环境	请从列表选择首选语言。

参数	描述
启用弹出通知	启用此选项表明要显示系统通知消息。要禁用系统通知，请将其关闭。

4. 单击**保存**。

查看用户登录历史记录

您可以查看用户的登录历史记录，以确定其帐户是否有未经授权的访问。您可以启用和禁用登录尝试跟踪，以及指定保留期来跟踪登录尝试。

关于此任务

如果启用登录历史记录显示，那么**登录历史记录**窗口将显示最后一次成功登录的日期、时间和 IP 地址，以及自最后一次成功登录以来用户的不成功登录尝试次数。

如果您指定保留期来跟踪登录尝试，那么 QRadar 会将登录历史记录保留所选天数。

过程

1. 在导航菜单（☰）上，单击**管理**。
2. 在**系统配置**部分中，单击**系统设置**。
3. 在**显示登录历史记录**字段中，选择 **True**。
4. 在**登录历史记录保留时间（天）**字段中，选择保留用户不成功登录尝试历史记录的天数。

   注: 缺省值为 0，这将保留所有的登录历史记录。
5. 单击**保存**。
6. 关闭“**系统设置**”窗口。
7. 在**管理**选项卡上，单击**部署更改**。

创建用户帐户

新建用户帐户时，必须为用户分配访问凭证、用户角色和安全概要文件。用户角色定义用户有权执行的操作。安全概要文件定义用户有权访问的数据。

开始之前

在您可以创建用户帐户之前，必须确保已创建必需的用户角色和安全概要文件。

关于此任务

您可以创建多个包含管理特权的用户帐户；但是，任何具有管理员经理特权的用户角色都可以创建其他管理用户帐户。

过程

1. 在导航菜单（☰）上，单击**管理**。
2. 在**用户管理**部分，单击**用户**。

   “**用户管理**”窗口将打开。
3. 单击**添加**。
4. 输入以下参数的值:

参数	描述
用户名	为新用户输入唯一用户名。用户名必须包含 1 - 60 个字符。

参数	描述
用户描述	为用户输入描述。描述不能包含超过 2048 个字符。
电子邮件	输入要与此用户关联的电子邮件地址。地址不能包含超过 255 个字符，而且不能包含空格。
新密码	输入使用户能够获取访问权的新密码。密码必须满足密码策略强制实施的最小长度和复杂性需求。
确认新密码	再次输入新密码。
用户角色	从列表中为此用户选择角色。
安全概要文件	从列表中为此用户选择安全概要文件。

5. 单击**保存**。
6. 关闭“**用户管理**”窗口。
7. 在**管理**选项卡上，单击**部署更改**。

编辑用户帐户

您可以通过主要产品界面编辑当前用户的帐户信息。要在“**用户管理**”窗口上快速找到要编辑的用户帐户，请在工具栏上的**搜索用户**文本框中输入用户名。

过程

1. 在导航菜单（☰）上，单击**管理**。
2. 在**用户管理**部分，单击**用户**。
3. 在“**用户管理**”窗口中，选择要编辑的用户。
   您可以使用**高级过滤器**以按用户角色或安全概要文件搜索。
4. 在“**用户详细信息**”窗口中，单击**编辑**。
5. 编辑用户的帐户信息。

参数	描述
用户描述	为用户输入描述。描述不能包含超过 2048 个字符。
电子邮件	输入要与此用户关联的电子邮件地址。地址不能包含超过 255 个字符，而且不能包含空格。
新密码	输入使用户能够获取访问权的新密码。密码必须满足密码策略强制实施的最小长度和复杂性需求。
确认新密码	再次输入新密码。
用户角色	从列表中为此用户选择角色。
安全概要文件	从列表中为此用户选择安全概要文件。

6. 单击**保存**。
7. 关闭“**用户管理**”窗口。
8. 在**管理**选项卡上，单击**部署更改**。

禁用用户帐户

您可以禁用用户帐户以限制用户访问 QRadar。用于禁用用户帐户的选项会临时撤销用户的访问权，而不删除此帐户。

关于此任务

如果禁用了帐户的用户尝试登录，系统会显示一条消息，向用户告知用户名和密码不再有效。用户创建的诸如已保存搜索和报告的项将仍然与其关联。

过程

1. 在导航菜单（☰）上，单击**管理**。
2. 在**用户管理**部分，单击**用户**。
3. 在“**用户管理**”窗口中，选择要禁用的用户帐户。
   您可以使用**高级过滤器**以按用户角色或安全概要文件搜索。
4. 单击**编辑**。
5. 从“**用户详细信息**”窗口，选择**用户角色**列表中的**已禁用**。
6. 单击**保存**。
7. 关闭“**用户管理**”窗口。
8. 在**管理**选项卡上，单击**部署更改**。

删除用户帐户

如果不再需要用户帐户，可以将其删除。删除用户后，用户无法再访问用户界面。如果用户尝试登录，系统会显示一条消息，向用户告知用户名和密码不再有效。

关于此任务

要在“**用户管理**”窗口上快速找到要删除的用户帐户，请在**搜索**文本框中输入用户名。

过程

1. 在导航菜单（☰）上，单击**管理**。
2. 在**用户管理**部分，单击**用户**。
3. 在“**用户管理**”窗口中，选择要删除的用户。
   您可以使用**高级过滤器**以按用户角色或安全概要文件搜索。
4. 在“**用户详细信息**”窗口中，单击**删除**。
   将开始进行从属项的搜索。
5. 在“**找到的从属项**”窗口中，**删除**或**重新分配**从属项。
6. 用户没有任何从属项时，单击**删除用户**。
7. 在“**确认删除**”窗口中，单击**删除 > 确定**。
8. 单击**删除用户**。
9. 关闭“**用户管理**”窗口。
10. 在**管理**选项卡上，单击**部署更改**。

删除已删除用户的已保存搜索

如果不再需要已删除用户的已保存搜索，那么可删除这些搜索。

关于此任务

已删除用户创建的已保存搜索仍然与用户关联，直到您删除这些搜索为止。

过程

1. 在导航菜单 (☰) 上，单击**日志活动**或**网络活动**。
2. 单击**搜索** > **管理搜索结果**。
3. 单击**状态**列以对保存的搜索进行排序。
4. 选择状态为“错误！”的已保存搜索，并单击**删除**。

SAML 单点登录认证

安全性断言标记语言 (SAML) 是服务提供者 (SP) 和身份提供者 (IDP) 之间的认证和授权框架，其中使用数字签名的 XML 文档交换认证。服务提供者同意信任身份提供者以认证用户。然后，身份提供者生成认证断言，这指示用户已进行认证。

通过使用 SAML 认证功能，您可以轻松地将 QRadar 与公司身份服务器相集成来提供单点登录，并且消除了维护 QRadar 本地用户的需求。向身份服务器进行认证的用户可自动向 QRadar 进行认证。他们无需记录单独的密码或者在每次访问 QRadar 时输入凭证。

QRadar 完全兼容 SAML 2.0 Web SSO 概要文件作为服务提供者。其支持 SP 和 IDP 启动的单点登录和单点注销。

配置 SAML 认证

您可以配置 IBM QRadar 以使用安全性断言标记语言 (SAML) 2.0 单点登录框架进行用户认证和授权。

开始之前

要在 QRadar 中完成 SAML 配置，必须在身份提供者 (SAML) 服务器上生成 XML 元数据文件。

关于此任务

遵循这些步骤以在 QRadar 主机上配置 SAML 认证。完成此任务后，必须配置身份提供者才能使用 QRadar。

过程

1. 在**管理**选项卡上，单击**认证**。
2. 在**常规认证设置**窗口上，选择 **SAML 2.0** 作为**认证模块**。
3. 在**身份提供者配置**部分中，单击**选择元数据文件**，浏览到身份提供者创建的 XML 元数据文件，然后单击**打开**。
4. 在**服务提供者配置**部分中，输入**实体标识** URL。
5. 选择**名称标识格式**：
   - 未指定（缺省）
   - 持久
   - 电子邮件
   - X509SubjectName
   - WindowsDomainQualifiedName
   - kerberos

   提示: 使用**未指定**，除非身份提供者不支持。
6. 选择**请求绑定协议**：
   - HTTP-POST
   - HTTP-Redirect
7. 如果希望身份提供者对返回的断言进行签名，请针对**请求签署的断言**选择**是**。
8. 如果您希望使用 QRadar 证书对身份提供者返回的断言进行加密，请针对**请求加密断言**选择**是**。

注: 启用加密需要第 21 页的『安装不受限制的 SDK JCE 策略文件』。

9. 如果希望使用 QRadar 证书对认证请求进行签名，请针对**对认证请求进行签名**选择**是**。
10. 如果要在用户注销 QRadar 时使其从身份提供者自动注销，请针对**启用服务提供者启动的单点注销**选择**是**。

    提示: 仅当身份提供者支持时才可使用此选项。
11. 使用以下其中一种方法来配置证书以进行签名和解密：

选项	描述
使用提供的 QRadar_SAML 证书	使用工具提示中的链接以下载根证书，根 CA CRL，中间 CA 以及证书的中间 CA CRL，应该将这些项上载到身份提供者服务器的可信证书库。
添加新证书	单击**添加**，并遵循此主题中的指示信息以添加定制证书：第 19 页的『导入新证书以用于签名和解密』
续订或更新现有证书	如果 QRadar_SAML 证书已到期或即将到期，请单击**续订**以续订证书。单击**更新**以更新已到期或即将到期的定制证书。这些选项的显示取决于所使用的证书。

12. 选择以下其中一种方法以授权用户：

选项	描述
本地	必须创建本地 QRadar 用户，并在**用户管理器**中配置其角色和安全概要文件。
用户属性	在收到认证请求时，QRadar 使用 SAML 断言中提供的属性，自动创建本地用户。根据角色属性和安全概要文件属性的值分配角色和安全概要文件。必须在断言中提供这些属性，QRadar 中必须已存在角色和安全概要文件。 **注:** 使用具有“管理”能力的角色时，安全概要文件属性的值必须为 *Admin*。 **提示:** 在多租户环境中，还必须配置 *Tenant* 属性，以将用户分配给租户。如果未提供租户属性，那么不会将创建的用户分配给任何租户。

13. 单击**保存认证模块**。

    将自动下载 QRadar SAML 元数据文件。
14. 在**管理**选项卡上，单击**部署更改**。

下一步做什么

如果选择了**本地**授权，请转至第 11 页的『第 3 章 用户管理』以创建本地用户。如果选择了**用户属性**，请根据需要创建角色、安全概要文件和租户，然后进行部署。

配置 QRadar 后，必须使用保存的 XML 元数据文件配置身份提供者。

导入新证书以用于签名和解密

QRadar SAML 2.0 功能允许您将提供的 QRadar_SAML 证书以外的 x509 证书用于签名和加密。

过程

1. 对于**用于签名和加密的证书**，请单击**添加**。
2. 在**导入新证书**窗口中，为该证书输入**友好名称**。
3. 单击**浏览**以选择**专用密钥文件**，然后单击**打开**。
4. 单击**浏览**以选择**证书文件**，然后单击**打开**。
5. 如果要上载的证书有中间 CA，请单击**浏览**以选择**中间 CA 文件**，然后单击**打开**。
6. 如果该证书的根 CA 不是随操作系统一起预安装的公共根 CA，请单击**浏览**以选择**根 CA 文件**，然后单击**打开**。
7. 单击**上载**，以上载该证书。

使用 Microsoft Active Directory Federation Services 来设置 SAML

在 QRadar 中配置 SAML 之后，您可使用在该过程期间创建的 XML 元数据文件来配置身份提供者。此示例中包含指示信息，说明如何配置 Microsoft Active Directory Federation Services (AD FS)，以使用 SAML 2.0 单点登录框架与 QRadar 进行通信。

开始之前

要配置 AD FS 服务器，您必须先在 QRadar 中配置 SAML。然后，将您在该过程期间创建的 QRadar SAML XML 元数据文件，复制到可供 AD FS 服务器访问的位置。

过程

1. 在 AD FS 管理控制台上，选择**信赖方信任**文件夹。
2. 在**操作**侧边栏上，单击标准**信赖方信任**，然后单击**启动**。
   这将打开**添加信赖方信任**向导。
3. 在**选择数据源**窗口上，选择**从文件导入有关信赖方的数据**，浏览到 QRadar SAML XML 元数据文件，然后单击**打开**。
4. 单击**下一步**。
5. 输入**显示名称**，添加任何相关的**注释**，然后单击**下一步**。
6. 选择访问控制策略，然后单击**下一步**。
7. 配置您需要的任何其他选项，然后单击**下一步**。
8. 单击**关闭**。
9. 在**信赖方信任**文件夹中，选择您所创建的新信任，然后单击**编辑声明颁发策略**。
10. 单击**添加规则**。
11. 从**声明规则模板**菜单中选择**以声明方式发送 LDAP 特性**，然后单击**下一步**。
12. 输入**声明规则名称**，然后选择**特性存储**。
13. 选择要在断言中发送的属性，映射到相应的**传出声明类型**，然后单击**完成**。
14. 单击**添加规则**。
15. 从**声明规则模板**菜单中选择**转换传入声明**，然后单击**下一步**。
16. 配置以下选项：
    - 声明规则名称
    - 传入声明类型 - 请使用值 UPN
    - 传出声明类型 - 配置为 NameID
    - 传出 NameID 格式
17. 选择**传递所有声明值**，然后单击**完成**。
18. 如果您已配置 QRadar，以将提供的 QRadar_SAML 证书用于 SAML，请将先前下载的根 CA、中间 CA 和 CRL 文件复制到 Windows 服务器上的目录。然后，在 Windows OS 上，以管理员身份打开命令行窗口，并输入以下命令：

```
certutil -addstore -f ROOT <local_path>vault-qrd_ca.pem
certutil -addstore -f CA <local_path>QRadarSAML_ca.crt
certutil -addstore -f ROOT <local_path>QRadarSAML_ca.crl
certutil -addstore -f Root <local_path>vault-qrd_ca.crl
```

这些文件位于 /opt/qradar/ca/www。

安装不受限制的 SDK JCE 策略文件

加密技术的使用受美国法律管控。IBM Java Solution Developer Kits (SDKs) 包含强大但受限制的管辖区域策略文件。要支持加密 SAML 断言，必须首先使用 IBM QRadar 获取不受限制的管辖区域 Java 密码术扩展 (JCE) 策略文件。

过程

1. 在此处下载不受限制的 Java 密码术扩展 (JCE) 策略文件：
   https://www14.software.ibm.com/webapp/iwm/web/preLogin.do?source=jcesdk
2. 选择 **Java 5.0 SR16、Java 6 SR13、Java 6 SR5 (J9 VM2.6)、Java 7 SR4、Java 8 GA 和所有后续发行版**。
3. 选择 **IBM SDK 策略文件**。

   注: 您将重定向到与 Java 版本兼容的 SDK 中的策略文件。QRadar V7.3.2 使用 SDK 1.8。
4. 使用 IBM 用户标识和密码登录。
   如果不具有 IBM 用户标识和密码，那么需要注册。按照登录页面上注册链接中操作。
5. 系统提示时，选择适用于正使用的 Java 版本的压缩文件。
6. 单击**继续**以开始下载。
7. 将压缩文件解压缩。
   选择以下 JAR 文件：
   - local_policy.jar
   - US_export_policy.jar
8. 将文件置于以下目录：
   /store/configservices/staging/globalconfig/java_security
9. 单击**部署更改**。

SAML 认证故障诊断

使用下列信息，可以对搭配使用 SAML 2.0 与 QRadar 时的错误及问题进行故障诊断。

登录或注销失败

单点登录或单点注销失败时，请确保您上载到身份提供者的 QRadar SAML 元数据与最新部署的元数据（位于 https://*<yourqradarserverhostname>*/console/SAMLMetadata）匹配。此外，请确保您已将所选证书的根 CA 文件、根 CA CRL 文件、中间 CA 文件和中间 CA CRL 文件上载到 IDP 服务器证书库的适当位置。使用提供的 QRadar_SAML 证书时，您可从下列位置下载这些文件：

```
http://<yourqradarserverhostname>:9381/vault-qrd_ca.pem
http://<yourqradarserverhostname>:9381/QRadarSAML_ca.crt
http://<yourqradarserverhostname>:9381/vault-qrd_ca.crl
http://<yourqradarserverhostname>:9381/QRadarSAML_ca.crl
```

注: 如果您使用的是提供的 QRadar_SAML 证书，那么从备份复原 QRadar 之后，必须执行上述步骤。

帐户未获授权

某些配置问题可能会引起此错误：

此帐户无权访问 QRadar。从 SAML 身份提供者进行注销并使用授权帐户来登录。

如果您使用的是**本地**授权，请确保 SAML 断言中的 **NameID** 与现有的 QRadar 用户名匹配，而且已部署该用户。

如果您使用的是**用户属性**授权，请确保 SAML 断言中包含所配置的角色属性和安全概要文件属性，而且这些属性的值与 QRadar 中部署的现有角色和安全概要文件匹配。使用具备“管理员”能力的角色时，安全概要文件属性的值必须为 *Admin*。在多租户环境中，如果该断言中包含租户属性，请确保该属性的值与 QRadar 中现有的租户匹配。

日志文件

通过使用身份提供者服务器日志和 /var/log/qradar.error 日志，您可诊断许多其他问题。

复原系统登录以进行调查

要调查 SAML 2.0 的问题，您可复原 QRadar，以使用缺省系统登录。

将 /opt/qradar/conf/templates/login.conf 的内容复制到 /opt/qradar/conf/login.conf

或者，在 QRadar V7.3.2 FP2 和更低版本中，您可以编辑 /opt/qradar/conf/login.conf 文件并将

```
ModuleClass=com.q1labs.uiframeworks.auth.SAMLLoginModule
```

更改为

```
ModuleClass=com.q1labs.uiframeworks.auth.UserConfLoginModule
```

在 QRadar V7.3.2 FP3 和更高版本中：编辑 /opt/qradar/conf/login.conf 文件并将

```
ModuleClass=com.q1labs.uiframeworks.auth.configuration.SamlLoginConfiguration
```

更改为

```
ModuleClass=com.q1labs.uiframeworks.auth.configuration.LocalPasswordLoginConfiguration
```

清空浏览器缓存，然后以“管理员”用户身份登录。完成调查之后，请将该属性重新更改为 SAMLLoginModule，并再次清空浏览器缓存。

使用身份提供者登录之后无法联系 QRadar 控制台

请确保本地 DNS 服务器可以解析 QRadar 控制台的主机名。此外，请确保您的计算机可使用主机名来联系 QRadar 控制台。

IDP 服务器上的登录或注销失败

请检查 IDP 服务器日志，确定这些失败是否由 CRL 撤销检查中的错误所致。如果是这样，请将 QRadar_SAML 证书 CRL 导入到 IDP 服务器中，并确保 IDP 服务器可使用 HTTP 连接来联系 QRadar 控制台。

身份提供者证书已到期

身份提供者元数据文件中的证书到期后，您就会无法登录 QRadar，而且以下错误会出现在 /var/log/qradar.error 文件中：

```
com.q1labs.uiframeworks.auth.saml.metadata.DefaultMetadataServiceImpl:
[ERROR] NotAfter: <date>
java.security.cert.CertificateExpiredException:  NotAfter:
```

要解决此问题，请要求您的身份提供者更新元数据文件中的证书，然后在 QRadar 中重新配置 SAML，以使用新的 IDP 元数据文件。

QRadar_SAML 证书已到期

当 QRadar_SAML 证书即将到期时，将会显示 QRadar 系统通知。

在该证书到期之前，您必须予以更新。

1. 在**管理**选项卡上，单击**认证**。
2. 在**一般认证设置**窗口上，选择 **SAML 2.0** 来作为**认证模块**。
3. 单击**更新**，以更新 QRadar_SAML 证书。
4. 单击**保存认证模块**。

QRadar SAML 元数据文件会自动下载。

5. 单击工具提示中的链接，以下载 QRadar 根 CA 和中间 CA 证书以及 CRL 文件。
6. 在**管理**选项卡上，单击**部署更改**。
7. 将下列文件发送到 IDP 服务器，以部署更改。
   - QRadar 元数据文件
   - QRadar 根 CA 证书
   - QRadar 中间 CA 证书
   - CRL 文件

第三方证书已到期

您并非必须使用 QRadar 所随附的 QRadar_SAML 证书；您可使用自己的第三方证书。该证书即将到期时，将会显示 QRadar 系统通知。

在第三方证书到期之前，您必须更新现有的证书，或添加新证书。

1. 在**管理**选项卡上，单击**认证**。
2. 在**一般认证设置**窗口上，选择 **SAML 2.0** 来作为**认证模块**。
3. 单击**添加**或**更新**。
4. 单击**保存认证模块**。

   QRadar SAML 元数据文件会自动下载。
5. 单击工具提示中的链接，以下载 QRadar 根 CA 和中间 CA 证书以及该证书的 CRL 文件。
6. 在**管理**选项卡上，单击**部署更改**。
7. 将下列文件发送到 IDP 服务器，以部署更改。
   - QRadar 元数据文件
   - QRadar 根 CA 证书
   - QRadar 中间 CA 证书
   - CRL 文件

第 4 章 系统管理

IBM QRadar 具有一个模块化体系结构，支持大小和拓扑不同的部署。

在单主机部署中，所有软件组件在单个设备上运行，并且 QRadar Console 提供用户界面、实时事件和流视图、报告、攻击、资产信息以及管理功能。

要扩展 QRadar，您可以将非控制台管理的主机添加到部署。您可以为每个受管主机配置特定组件类型，例如，数据网关、处理器和数据节点，从而提供更大的灵活性来管理分布式环境中的数据收集和处理。

相关概念

IBM QRadar 产品中的功能

查看系统运行状况信息

QRadar Deployment Intelligence 应用程序是功能强大的监视应用程序，其整合部署中每个受管主机的历史运行状况数据。使用应用程序可监视 QRadar 部署的运行状况。

QRadar Deployment Intelligence 上的 **主机状态概述**仪表板显示每个设备的状态（活动、备用、脱机或未知）以及每个主机的通知数量、主机名和设备类型、磁盘使用情况、状态和更改时间。您可以从**主机状态概述**向下钻取，以查看有关受管主机状态的更多直观信息，包括事件和流速率、系统通知和磁盘信息。

为帮助对环境中的问题进行故障诊断，请使用**获取日志**功能以从 QRadar Console 和部署中的任何其他受管主机收集日志文件。

QRadar Deployment Intelligence 应用程序位于 IBM Security App Exchange 上。您必须安装应用程序，然后创建授权服务令牌来允许应用程序使用 QRadar API 以从受管主机请求数据。

QRadar Deployment Intelligence 应用程序使用 QRadar 运行状况度量来监视部署。运行状况度量是不计入许可证的基本、轻量级系统事件。

QRadar 组件类型

添加到部署的每个 IBM QRadar 设备具有可配置组件，这些组件指定受管主机在 QRadar 中的行为方式。

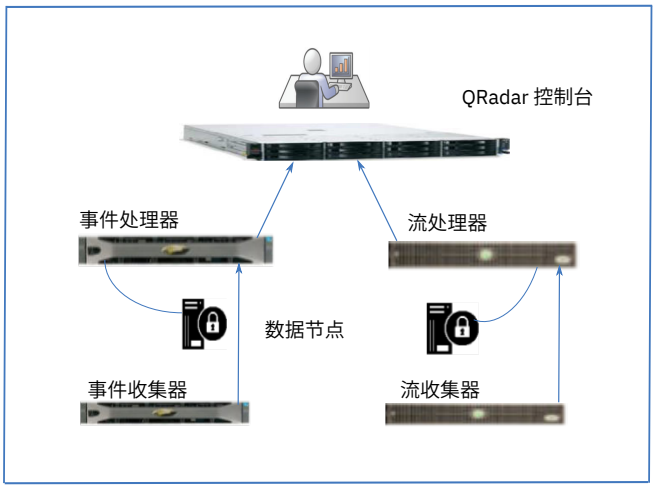

图 *4. QRadar* 事件和流组件

QRadar Console

QRadar Console 提供 QRadar 产品界面、实时事件和流视图、报告、攻击、资产信息和管理功能。在分布式环境中，使用 QRadar Console 来管理部署中的其他组件。

事件收集器

事件收集器 从本地和远程日志源收集事件，并规范化原始事件数据，从而可供 QRadar 使用。为节约系统资源，事件收集器 将相同事件绑定在一起并将数据发送到事件处理器。

事件处理器

事件处理器处理从一个或多个 事件收集器 组件收集的事件。如果将事件匹配到在控制台上定义的定制规则，那么事件处理器执行在规则响应中定义的操作。

每个事件处理器都具有本地存储器。事件数据存储在处理器上，或者可存储在 数据节点 上。

QRadar QFlow Collector

QRadar QFlow Collector 从网络上的设备收集网络流。包含活动和记录的订阅源，例如，网络分流器、跨端口、NetFlow 和 QRadar 流日志。

限制: QRadar Log Manager 不支持流集合。

流处理器

流处理器 处理来自一个或多个 QRadar QFlow Collector 设备的流。流处理器 设备还可以直接从网络中的路由器收集外部网络流，例如，NetFlow、J-Flow 和 sFlow。

流处理器 包含板载处理器和内部存储器以用于流数据。

数据节点

数据节点 接收来自事件和流处理器的安全事件和流，并将数据存储到磁盘。

数据节点 始终连接到事件处理器或 流处理器。

非现场源和目标设备

非现场设备是不属于 QRadar Console 监视的部署的 QRadar 设备。

非现场源设备将规范化数据转发到 事件收集器。您可以配置非现场源以在转发前加密数据。

非现场目标设备接收来自任何 事件收集器 或环境中的任何处理器的规范化事件或流数据。

更高版本的 QRadar 系统可接收来自更低版本的 QRadar 系统的数据，但是较低版本无法接收来自较高版本的数据。为避免出现问题，请在升级发送方前升级所有接收方。

数据节点

数据节点是您添加到事件和流处理器以增加存储容量和提升搜索性能的设备。您可向 IBM QRadar 部署添加的数据节点数量并无限制，并且可随时添加。每个数据节点都只能连接到一个处理器，但处理器可支持多个数据节点。

有关部署规划的更多信息，请参阅：*IBM QRadar* 体系结构和部署指南。

QRadar 系统时间

在部署跨多个时区时，配置所有应用程序以使用与 IBM QRadar 控制台相同的时区。此外，您可以配置所有设备以使用格林威治标准时间 (GMT)。

从 QRadar 用户界面配置 IBM QRadar 系统时间。您可以手动配置时间，或者通过配置网络时间协议 (NTP) 服务器来维护系统时间。

将在 QRadar Console 和受管主机之间自动同步时间。

时区不匹配所导致的问题

为确保搜索和数据相关功能正常运行，所有设备必须与 QRadar Console 设备同步时间设置。在时区设置不匹配时，您可能会在 QRadar 搜索和报告数据之间看到不一致的结果。

累加器服务在具有本地存储器的所有设备上运行，以创建逐分钟累积，以及每小时和每天累积。QRadar 在报告和时间序列图中使用累积的数据。如果分布式环境中的时区不匹配，那么在与 AQL 查询结果进行比较时，报告和时间序列图形可能显示不一致的结果，这是由于汇总累积数据的方式。

QRadar 搜索针对 Ariel 数据库中存储的数据运行，此数据库使用日期结构 (YYYY/MM/DD/HH/MM) 以将文件存储到磁盘。在数据写入到磁盘后更改时区会破坏 Ariel 数据库中的文件命名序列，并且可能导致数据完整性问题。

支持 NAT 的 网络

网络地址转换 (NAT) 将一个网络中的 IP 地址转换为另一个网络中的不同 IP 地址。NAT 针对 IBM QRadar 部署提供增强的安全性，因为通过转换处理管理请求并且隐藏内部 IP 地址。利用 NAT，位于专用内部网络上的计算机可通过网络设备（通常是防火墙）进行转换，并且可通过此网络与公共因特网进行通信。使用 NAT 以将单个内部 IP 地址映射到单个外部 IP 地址。

QRadar NAT 配置需要静态 NAT 并且每个受管主机仅允许一个公用 IP 地址。

不在同级的相同 NAT 组中或者位于不同 NAT 组中的任何 QRadar 主机都将配置为使用此主机的公用 IP 地址以进行访问。例如，在 QRadar Console 上配置公用 IP 地址时，位于相同 NAT 组中的任何主机使用 QRadar Console 的专用 IP 地址以进行通信。位于不同 NAT 组中的任何受管主机使用 QRadar Console 的公用 IP 地址以进行通信。

如果在不需要外部转换的其中一个 NAT 组位置中有一个主机，请在**专用 IP** 和**公用 IP** 字段中输入专用 IP 地址。NAT 组与控制台不同的远程位置中的系统将需要一个额外的 IP 地址和 NAT，因为需要能够建立到控制台的连接。仅位于与控制台相同的 NAT 组中的主机可使用相同公用和专用 IP 地址。

受管主机

为提高数据收集以及事件和流处理的灵活性，通过添加非控制台受管主机（例如，网关、处理器和数据节点），构建分布式 IBM QRadar 部署。

有关规划和构建 QRadar 环境的更多信息，请参阅 *IBM QRadar* 体系结构和部署指南。

软件兼容性需求

环境中所有 IBM QRadar 设备的软件版本必须位于相同版本和修订包级别。不支持使用不同版本的软件的部署，因为混合软件环境可能导致不触发规则、不创建或更新攻击以及搜索结果错误。

在受管主机使用与 QRadar 控制台不同的软件版本时，您能够查看已分配给主机的组件，但是无法配置组件或者添加或分配新组件。

因特网协议 (IP) 需求

在添加非控制台受管主机时，支持不同的 IP 协议组合，如下表中所述：

表 3. 添加非控制台受管主机时受支持的 *IP* 协议组合

受管主机	QRadar 控制台（IPv6，单个）	QRadar 控制台（IPv6，HA）	QRadar 控制台（双堆栈，单个）	QRadar 控制台（双堆栈，HA）
IPv4，单个	×	×	√*	×
IPv4，HA	×	×	×	×
IPv6，单个	√	√	√	×
IPv6，HA	√	√	√	×

限制: *缺省情况下，无法向 IPv6 和 IPv4 双堆栈控制台添加仅限 IPv4 受管主机。必须运行脚本以启用仅限 IPv4 的受管主机。有关更多信息，请参阅在双堆栈环境中添加仅限 IPv4 受管主机。

双堆栈控制台是支持 IPv4 和 IPv6 的控制台。

无法向双堆栈 HA 控制台添加受管主机。

可以向双堆栈单个控制台或向仅限 IPv6 控制台添加 IPv6 受管主机。

只能向双堆栈单个控制台添加 IPv4 受管主机。

受管主机的带宽注意事项

要复制状态和配置数据，请确保在 IBM QRadar 控制台和所有受管主机之间至少具有 100 Mbps 的带宽。在搜索日志和网络活动时需要更高的带宽，而您具有的每秒事件数 (EPS) 在 10,000 以上。

配置为将数据存储转发到事件处理器的 事件收集器 根据设置的调度来转发数据。请确保您具有足够的带宽来覆盖收集的数据量，否则转发设备无法维持计划的步调。

使用以下方法缓解数据中心之间的带宽限制：

在主数据中心处理数据并将其发送到主机

将部署设计为在控制台驻留的主数据中心处理收集的数据并将其发送到主机。在此设计中，所有基于用户的搜索都从本地数据中心查询数据，而不是等待远程站点发回数据。

您可以在远程位置部署存储转发事件收集器（例如 QRadar 15XX 物理或虚拟设备），以控制整个网络的数据脉冲串。带宽用于远程位置中，并且数据搜索发生在主数据中心而不是远程位置。

不要在带宽有限的连接上运行数据密集型搜索

确保用户不要在带宽有限的链路上运行数据密集型搜索。指定精确搜索过滤器会限制从远程位置收集的数据量，并减少发回查询结果所需的带宽。

加密

为在环境中的每个设备之间提供安全数据传输，IBM QRadar 集成了使用 OpenSSH 的加密支持。在受管主机之间发生加密；因此，您必须至少具有一个受管主机，然后才能启用加密。

在启用加密时，将使用 SSH 协议连接在启动连接的客户机上创建一个安全通道。在受管主机上启用加密时，将针对受管主机上的所有客户机应用程序创建一个 SSH 隧道。在非控制台受管主机上启用加密时，将自动针对数据库和到控制台的其他支持服务连接创建加密隧道。要确保加密受管主机之间的所有数据，请启用加密。

例如，在事件处理器上启用加密时，事件处理器和 事件收集器 之间的连接进行加密，并且 事件处理器 和 Magistrate 之间的连接也进行加密。

两个受管主机之间的 SSH 隧道可以从远程主机而不是本地主机启动。例如，如果您已建立从安全环境中的事件处理器到安全环境外的事件收集器的连接，并有将阻止您将安全环境外的主机连接到安全环境中的主机的防火墙规则，那么您可以通过为事件收集器选中**远程隧道启动**复选框来切换创建此隧道的主机以便从事件处理器建立连接。

您不能将隧道从控制台反转到受管主机。

在 QRadar 环境中执行更改

对 IBM QRadar 执行配置更改时，更改会保存至登台区域，“**管理**”选项卡上的部署条幅会更新以指示需要部署更改。部署更改可能需要重新启动 QRadar 服务。

QRadar 有两种部署更改的方法：标准和完整配置。所需的部署类型取决于所执行的更改类型。

标准部署

此部署方法仅重新启动受执行的更改直接影响的服务。单击“**管理**”选项卡条幅上的**部署更改**开始标准部署。

以下列表显示了需要标准部署的更改示例：

- 添加或编辑新用户或用户角色。
- 为其他用户设置密码。
- 更改用户角色或安全概要文件。

完整配置部署

影响整个 QRadar 部署的更改必须使用完整配置部署方法进行部署。通过单击“**管理**”选项卡上的**高级**菜单中的**部署完整配置**开始完整配置部署。

此方法会在每个受管主机上重新构建所有配置文件。为确保正确装入新配置，受管主机上的所有服务都会自动重新启动（事件收集服务除外）。当其他服务重新启动时，QRadar 会继续收集事件并将其存储在缓冲区内直至受管主机恢复联机。

以下列表显示了需要完整配置部署的更改示例：

- 添加受管主机。
- 更改受管主机配置。
- 配置非现场主机，以向 QRadar Console 发送数据或从中接收数据。
- 复原配置备份。

更改影响事件集合

事件通过 ecs-ec-ingress 事件收集服务进入 QRadar。从 QRadar V7.3.1 开始，此服务的管理与其他 QRadar 服务相分离。为最大程度减少收集事件数据的中断，在 hostcontext 服务重新启动时，此服务不会自动重新启动。

以下情况可能会导致事件收集中断：

· 重新引导收集事件的设备。

· 添加 HA 受管主机。

· 在 HA 故障转移期间。

· 复原配置备份。

· 添加或移除非现场源连接

· 在分区的磁盘使用量超过最大阈值时。

在复原配置备份后部署发生更改时，您可以立即或稍后重新启动事件收集服务。在选择稍后重新启动服务时，QRadar 部署不依赖于事件收集服务的所有更改，并且在其他服务重新启动时继续收集事件。部署条幅继续显示未部署的更改，并且在查看详细信息时显示必须重新启动事件收集服务消息。

配置 事件收集器

在想要扩展部署时添加 QRadar 事件收集器 以收集更多本地事件或者从远程位置收集事件。

过程

1. 在导航菜单（☰）上，单击**管理**。
2. 单击**系统配置 > 系统和许可证管理**。
3. 选择要配置的受管主机。
4. 单击**部署操作 > 编辑主机**。
5. 单击**组件管理**。
6. 输入以下参数的值：

参数	描述
事件转发侦听端口	事件收集器 事件转发端口。
流转发侦听端口	事件收集器 流转发端口。
启用自动检测	**True**：使 事件收集器 自动分析和接受来自先前未知日志源的流量。相应的防火墙端口已打开以启用“自动检测”，才能接收事件。此选项是缺省值。 **False**：阻止 事件收集器 自动分析和接受来自先前未知源的流量。 有关更多信息，请参阅《*Managing Log Sources Guide*》。
自动检测 - 使用全局设置	**True**：指定针对“日志源自动检查”，事件收集器使用全局设置。 **False**：指定针对“日志源自动检查”，事件收集器 使用单个本地设置（XML 配置文件）。
启用流重复数据删除	
流重复数据删除过滤器时间	流在转发之前缓冲的时间（秒）。
非对称流过滤器事件	非对称流在转发之前缓冲的时间（秒）。

参数	描述
转发已看到的事件	**True**：使 事件收集器 转发在系统上检测到的事件。 **False**：阻止 事件收集器 转发在系统上检测到的事件。此选项可防止在系统上出现事件循环。
压缩事件处理器流量	

7. 单击**保存**。
8. 针对要配置的部署中所有 QRadar Event Collector 重复操作。

部署更改

必须将对 IBM QRadar 部署进行的更改从登台区域推送到生产区域。

过程

1. 在导航菜单（☰）上，单击**管理**。
2. 检查部署条幅以确定是否必须部署更改。
3. 单击**查看详细信息**，以查看有关未部署配置更改的信息。
4. 选择部署方法：
   a) 要部署更改且仅重新启动受影响的服务，请在部署条幅上单击**部署更改**。
   b) 要重建配置文件并重新启动每个受管主机上所有服务，请单击**高级 > 部署完整配置**。

   注: QRadar 在您部署完整配置时会继续收集事件。事件收集服务必须重新启动的情况下，QRadar 并不会将其自动重新启动。将显示一条消息，为您提供选项以取消部署并在更方便的时候重新启动服务。

重新启动事件收集服务

可能存在想要仅重新启动 IBM QRadar 环境中所有受管主机上的事件收集服务的情况。例如，在新版本的 **ecs-ec-ingress** 服务可升级时，或者在先前部署期间延迟重新启动服务时。

过程

1. 在导航菜单（☰）上，单击**管理**。
2. 在**高级**菜单上，单击**重新启动事件收集服务**。在服务重新启动时，事件收集短暂中断。

重置 SIM

调整您的部署之后，通过重置 SIM 以从数据库和磁盘中移除所有的攻击以及源和目标 IP 地址，可以避免接收任何其他误报信息。

关于此任务

根据系统中的数据量，SIM 重置过程可能需要几分钟时间。在 SIM 重置过程期间，如果您尝试移至 IBM QRadar 用户界面的其他区域，那么会显示错误消息。

过程

1. 在导航菜单（☰）上，单击**管理**。
2. 从**高级**菜单中，选择**清除 SIM 模型**。
3. 阅读“**重置 SIM 数据模型**”窗口上的信息。
4. 选择下列其中一个选项：

选项	描述
软清除	用于关闭数据库中的所有攻击。如果您选中**软清除**选项，那么还可以选中**取消激活所有的攻击**复选框。
硬清除	从数据库中清除所有当前和历史 SIM 数据，包括受保护的攻击、源 IP 地址和目标 IP 地址。

5. 如果您要继续，请选中**是否确实要重置数据模型？**复选框。
6. 单击**继续**。
7. 当 SIM 重置过程完成后，单击**关闭**。
8. 刷新 Web 浏览器。

第 5 章 设置 QRadar

使用“管理”选项卡上的设置以配置 IBM QRadar 部署，包括网络层次结构、自动更新、系统设置、事件保留存储区、系统通知、控制台设置和索引管理。

相关概念

IBM QRadar 产品中的功能

网络层次结构

IBM QRadar 使用网络层次结构对象和组来查看网络中的网络活动以及监视组或服务。

在部署网络层次结构时，请考虑使用最高效方法来查看网络活动。网络层次结构不必与网络的物理部署类似。QRadar 支持可由 IP 地址范围定义的任何网络层次结构。您可以使网络基于多个不同的变量，包括地理位置或业务单位。

相关概念

多租户部署中的网络层次结构更新

定义网络层次结构的准则

在 IBM QRadar 中构建网络层次结构是配置部署期间至关重要的第一步。如果未正确配置网络层次结构，那么 QRadar 无法确定流方向、构建可靠的资产数据库或者从规则中的有用构建块获益。

在定义网络层次结构时请考虑以下准则：

- 按角色或类似流量模式组织系统和网络。

  例如，您可以组织网络以包含邮件服务器、部门用户、实验室或开发团队的组。使用此组织，您可以区分网络行为和实施基于行为的网络管理安全策略。但是，不将具有独特行为的服务器与网络上的其他服务器分组在一起。单独放置独特服务器可在 QRadar 中提供更多的服务器可视性，并且更易于为服务器创建特定安全策略。

- 将高流量服务器（例如，邮件服务器）放置在组的顶部。该层次结构可在发生不一致时提供可视化表示。
- 请勿配置超过 15 个对象的网络组。

  大型网络组可能导致难于查看每个对象的详细信息。如果部署处理的流数量超过 600,000，那么考虑创建多个顶级组。

- 通过将多个无类别域间路由 (CIDR) 或子网组合到单个网络组，节约磁盘空间。

  例如，添加密钥服务器作为单个对象，并将其他主要但相关的服务器分组到多个 CIDR 对象。

表 *4.* 单个网络组中多个 *CIDR* 和子网的示例

组	描述	IP 地址
1	市场营销	10.10.5.0/24
2	销售	10.10.8.0/21
3	数据库集群	10.10.1.3/32 10.10.1.4/32 10.10.1.5/32

- 定义一个全方位组，从而在定义新网络时，可应用相应的策略和行为监视器。

  在以下示例中，如果将 HR 部门网络（例如，10.10.50.0/24）添加到 Cleveland 组，那么流量显示为基于 Cleveland，并且缺省情况下，应用于 Cleveland 组的任何规则将应用。

表 5. 全方位组的示例		
组	**子组**	**IP 地址**
Cleveland	Cleveland 杂项	10.10.0.0/16
Cleveland	Cleveland 销售	10.10.8.0/21
Cleveland	Cleveland 市场营销	10.10.1.0/24

· 在启用域的环境中，确保将每个 IP 地址分配给相应的域。

相关信息

QRadar Support Geodata 常见问题

可接受的 CIDR 值

IBM QRadar 接受特定 CIDR 值。

下表提供了 QRadar 接受的 CIDR 值列表：

表 6. 可接受的 *CIDR* 值			
CIDR 长度	**掩码**	**网络数量**	**主机**
/1	128.0.0.0	128 A	2,147,483,392
/2	192.0.0.0	64 A	1,073,741,696
/3	224.0.0.0	32 A	536,870,848
/4	240.0.0.0	16 A	268,435,424
/5	248.0.0.0	8 A	134,217,712
/6	252.0.0.0	4 A	67,108,856
/7	254.0.0.0	2 A	33,554,428
/8	255.0.0.0	1 A	16,777,214
/9	255.128.0.0	128 B	8,388,352
/10	255.192.0.0	64 B	4,194,176
/11	255.224.0.0	32 B	2,097,088
/12	255.240.0.0	16 B	1,048,544
/13	255.248.0.0	8 B	524,272
/14	255.252.0.0	4 B	262,136
/15	255.254.0.0	2 B	131,068
/16	255.255.0.0	1 B	65,534
/17	255.255.128.0	128 C	32,512
/18	255.255.192.0	64 C	16,256
/19	255.255.224.0	32 C	8,128
/20	255.255.240.0	16 C	4,064
/21	255.255.248.0	8 C	2,032
/22	255.255.252.0	4 C	1,016
/23	255.255.254.0	2 C	508

表 6. 可接受的 *CIDR* 值 *(续)*			
CIDR 长度	**掩码**	**网络数量**	**主机**
/24	255.255.255.0	1 C	254
/25	255.255.255.128	2 个子网	124
/26	255.255.255.192	4 个子网	62
/27	255.255.255.224	8 个子网	30
/28	255.255.255.240	16 个子网	14
/29	255.255.255.248	32 个子网	6
/30	255.255.255.252	64 个子网	2
/31	255.255.255.254	无	无
/32	255.255.255.255	1/256 C	1

例如，当前缀边界包含的位数少于自然（或有类）网络掩码的位数，那么此网络将被称为超网。当前缀边界包含的位数多余自然网络掩码的位数时，此网络被称为子网。

· 209.60.128.0 是 C 类网络地址，掩码为 /24。

· 209.60.128.0 /22 是超网，可生成：

  – 209.60.128.0 /24
  – 209.60.129.0 /24
  – 209.60.130.0 /24
  – 209.60.131.0 /24

· 192.0.0.0 /25

  子网主机范围

  0 192.0.0.1-192.0.0.126

  1 192.0.0.129-192.0.0.254

· 192.0.0.0 /26

  子网主机范围

  0 192.0.0.1 - 192.0.0.62

  1 192.0.0.65 - 192.0.0.126

  2 192.0.0.129 - 192.0.0.190

  3 192.0.0.193 - 192.0.0.254

· 192.0.0.0 /27

  子网主机范围

  0 192.0.0.1 - 192.0.0.30

  1 192.0.0.33 - 192.0.0.62

  2 192.0.0.65 - 192.0.0.94

  3 192.0.0.97 - 192.0.0.126

  4 192.0.0.129 - 192.0.0.158

  5 192.0.0.161 - 192.0.0.190

  6 192.0.0.193 - 192.0.0.222

7 192.0.0.225 - 192.0.0.254

相关任务

定义网络层次结构

IBM QRadar 中包含了具有预定义网络组的缺省网络层次结构。您可以编辑预定义网络层次结构对象，或可以创建新的网络组或对象。

定义网络层次结构

IBM QRadar 中包含了具有预定义网络组的缺省网络层次结构。您可以编辑预定义网络层次结构对象，或可以创建新的网络组或对象。

关于此任务

网络对象是无类域间路由 (CIDR) 地址的容器。在网络层次结构中 CIDR 范围中定义的任何 IP 地址被视为本地地址。在网络层次结构中 CIDR 范围中未定义的任何 IP 地址被视为远程地址。一个 CIDR 只能属于一个网络对象，但是一个 CIDR 范围的子集可属于另一个网络对象。网络流量与最准确的 CIDR 匹配。一个网络对象可以分配多个 CIDR 范围。

QRadar 中的部分缺省构建块和规则使用缺省网络层次结构对象。更改缺省网络层次结构对象之前，搜索规则和构建块，以了解如何使用对象，以及在修改对象后可能需要调整哪些规则和构建块。请务必保持网络层次结构、规则和构建块最新以防止欺诈攻击。

过程

1. 在导航菜单（☰）上，单击**管理**。
2. 在**系统配置**部分中，单击**网络层次结构**。
3. 从“**网络视图**”窗口上的菜单树，选择要在其中操作的网络区域。
4. 要添加网络对象，请单击**添加**并完成以下字段：

选项	描述
名称	网络对象的唯一名称。 **提示:** 您可以在网络对象名称中使用句点来定义网络对象层次结构。例如，如果输入对象名称 D.E.F，即会创建三层层次结构，其中 E 作为 D 的子节点，F 作为 E 的子节点。
组	要在其中添加网络对象的网络组。从**组**列表选择，或单击**添加新组**。 **提示:** 添加网络组时，可在网络组名称中使用句点以定义网络组层次结构。例如，如果输入组名 A.B.C，即会创建三层层次结构，其中 B 作为 A 的子节点，C 作为 B 的子节点。
IP/CIDR(s)	输入网络对象的 IP 地址或 CIDR 范围，并单击**添加**。您可以添加多个 IP 地址和 CIDR 范围。
描述	网络对象的描述。此字段是可选的。
国家或地区	网络对象所在的国家/地区。此字段是可选的。
经度和纬度	网络对象的地理位置（经度和纬度）。这些字段相互依赖，且为可选字段。

5. 单击**创建**。
6. 重复这些步骤以添加更多网络对象，或者单击**编辑**或**删除**以使用现有网络对象。

相关概念

可接受的 CIDR 值

IBM QRadar 接受特定 CIDR 值。

IF-MAP 服务器证书

元数据访问点接口 (IF-MAP) 规则响应使 IBM QRadar Console 能够将从事件、流和攻击派生的警报和攻击数据发布至 IF-MAP 服务器。

配置 IF-MAP 服务器证书以进行基本认证

此任务提供有关如何配置 IF-MAP 证书以进行基本认证的指示信息。

开始之前

请联系 IF-MAP 服务器管理员以获取 IF-MAP 服务器公用证书的副本。证书必须具有 `.cert` 文件扩展名。

过程

1. 使用 SSH 以 root 用户身份登录到 IBM QRadar。
2. 将证书复制到 `/opt/qradar/conf/trusted_certificates` 目录。

SSL 证书

安全套接字层 (SSL) 是 Web 站点用于保护网上交易的行业标准安全协议。其提供通信隐私，因此客户机/服务器应用程序可在防窃听、篡改和消息伪造方式下通信。要生成 SSL 链接，Web 服务器需要 SSL 证书。SSL 证书由内部或信任的第三方认证中心发布。

浏览器和操作系统包含预先安装的可信证书列表，这些证书安装在受信任的根证书颁发机构存储库中。

自签名证书

自签名证书提供基本安全性，支持用户和应用程序之间的数据加密。因为任何现有已知根证书机构无法认证自签名证书，因此用户将收到有关此未知证书的警告并且必须接受才能继续。

内部 CA 签名的证书

具有自己的内部根证书机构 (CA) 的组织可使用此内部 CA 创建证书。QRadar 支持此证书，并且内部根 CA 也将导入到 QRadar 环境。

签名的公共 CA/中间 CA

QRadar 支持已知公共 CA 签署的证书和中间证书。

可直接在 QRadar 中使用公共签名证书，并且将使用签名证书和中间证书安装使用中间 CA 签名的证书，从而提供有效的证书功能。

注: 在环境中创建多个 SSL 密钥并且想要已知商业证书供应商进行签名的组织通常使用中间证书。在使用中间密钥时，可从此中间密钥创建子密钥。使用此配置时，必须使用中间证书和主机 SSL 证书配置 QRadar，从而使到主机的连接可验证完整的证书路径。

QRadar 组件之间的 SSL 连接

要在组件之间建立所有内部 SSL 连接，QRadar 使用在 QRadar 控制台上预先安装的 Web 服务器证书。

QRadar 的所有可信证书必须满足以下需求:

- 证书必须是 X.509 证书并且采用 PEM base64 编码。
- 证书必须具有 `.cert`、`.crt`、`.pem` 或 `.der` 文件扩展名。
- 包含证书的密钥库文件必须具有 `.truststore` 文件扩展名。
- 证书文件必须存储在 `/opt/qradar/conf/trusted_certificates` 目录中。

QRadar 部署中的 IPv6 寻址

针对 IBM QRadar 软件和设备的网络连接与管理支持 IPv4 和 IPv6 寻址。安装 QRadar 时，系统会提示您指定因特网协议为 IPv4 还是 IPv6。

支持 IPv6 寻址的 QRadar 组件

以下 QRadar 组件支持 IPv6 寻址。

网络活动选项卡

由于 **IPv6 源地址**和 **IPv6 目标地址**不是缺省列，因此不会自动显示这些列。要显示这些列，必须在配置搜索参数（列定义）时选中这些列。

为在 IPv4 或 IPv6 源环境中节省空间和建立索引，不存储或显示额外的 IP 地址字段。在混合 IPv4 和 IPv6 环境中，流记录包含 IPv4 和 IPv6 地址。

针对包数据（包括 sFlow）和 NetFlow V9 数据均支持 IPv6 地址。但是，较低版本的 NetFlow 可能不支持 IPv6。

日志活动选项卡

由于 **IPv6 源地址**和 **IPv6 目标地址**不是缺省列，因此不会自动显示这些列。要显示这些列，必须在配置搜索参数（列定义）时选中这些列。

DSM 可解析来自事件有效内容的 IPv6 地址。如果任何 DSM 无法解析 IPv6 地址，那么日志源扩展可解析这些地址。有关日志源扩展的更多信息，请参阅《《*DSM* 配置指南》》。

对 IPv6 字段进行搜索、分组和报告

您可以通过在搜索条件中使用 IPv6 参数来搜索事件和流。

您还以对基于 IPv6 参数的事件和流记录进行分组和排序。

您可以基于来自基于 IPv6 的搜索的数据创建报告。

定制规则

在定制规则和构建块中，IP 参数支持 IPv4 和 IPv6 地址，除非这些参数被标记为只能使用其中之一（例如，**SRC IPv6** 仅支持 IPv6 地址）。

设备支持模块 (DSM)

DSM 可解析来自事件有效内容的 IPv6 源和目标地址。

在 IPv6 或混合环境中部署 QRadar

要在 IPv6 或混合环境中登录至 QRadar，请使用方括号将 IP 地址括起。例如，`https://[<IP Address>]`

IPv4 和 IPv6 环境均可使用主机文件进行地址转换。在 IPv6 或混合环境中，客户机按控制台的主机名来解析其地址。必须将 IPv6 控制台的 IP 地址添加到客户机上的 `/etc/hosts` 文件中。

接受来自 IPv4 和 IPv6 地址的流源（例如，NetFlow 和 sFlow）。接受来自 IPv4 和 IPv6 地址的事件源（例如，系统日志和 SNMP）。您可以禁用 IPv6 环境中的超流和流绑定。

限制: 缺省情况下，不能将仅限 IPv4 的受管主机添加到 IPv6 和 IPv4 混合方式控制台中。必须运行脚本以启用仅限 IPv4 的受管主机。

IPv6 寻址限制

在 IPv6 环境中部署 QRadar 时，已知存在以下限制：

· 一部分 QRadar 部署无法充分利用启用 IPv6 的网络层次结构，包括监控、搜索和分析。

· 在定制规则中不存在针对 IPv6 地址的主机概要文件测试。

· 不存在 IPv6 地址的专用索引或优化。

高级 iptables 规则示例

您可配置 iptables 规则以便更好地控制对 QRadar 的访问、限制入站数据源并重定向流量。以下示例可帮助您通过手动调整 iptables 来获取对网络的更清晰的洞察。

阻止对 SSH 的 iptables 访问

控制台和不受管的主机允许从任何入站请求通过 SSH 进行连接。将主机添加到部署中时，控制台会允许来自 QRadar Console 的 SSH 访问，并且控制台会保持端口 22 处于打开状态，以便用于入站连接。您可通过修改主机的 iptables 规则来限制端口 22 上的入站连接。

您可在控制台上阻止来自其他受管主机的 SSH 访问，这样会中断加密连接。

```
-A INPUT -i eth0 -m state --state NEW -m tcp -p tcp --dport 22 -s 10.100.50.41 -j ACCEPT
-A INPUT -i eth0 -m state --state NEW -m tcp -p tcp --dport 22 -s 10.100.50.59 -j ACCEPT
-A INPUT -i eth0 -m state --state NEW -m tcp -p tcp --dport 22 -j DROP
```

启用到 QRadar 系统的 ICMP

您可通过将以下规则添加到 `/opt/qradar/conf/iptables.pre` 文件中，以便从 QRadar 系统启用 ping 响应。

```
-A INPUT -p icmp -j ACCEPT
```

运行以下脚本以在 `/etc/sysconfig/iptables` 文件中创建条目。

要点: 您可通过添加 `-s source.ip.address` 字段来将此规则限制于特定主机。

阻止不需要的数据源

您可短期阻止数据源（如日志源或 netflow 数据源），而无需禁用原始设备。要阻止特定主机，可将如下条目添加到 `/opt/qradar/conf/iptables.pre` 中。

阻止来自路由器的 netflow:

```
-A INPUT -p udp -s <IP Address> --dport 2055 -j REJECT
```

阻止来自其他源的 syslog:

```
-A INPUT -p tcp -s <IP Address> --dport 514 -j REJECT
-A INPUT -p udp -s <IP Address> --dport 514 -j REJECT
```

阻止来自特定子网的 syslog:

```
-A INPUT -p tcp -s <IP Address> --dport 514 -j REJECT
-A INPUT -p udp -s <IP Address> --dport 514 -j REJECT
```

配置 iptables 规则

对 QRadar 网络服务的访问权首先通过 iptables 在主机上进行控制。根据部署需求对 iptables 规则调整和配置。Ariel 端口搜索、流式操作以及使用加密（隧道化）的次数都可更新多个 iptables 规则。

关于此任务

您可以配置和检查适用于 IPv4 和 IPv6 的 iptables 规则。以下过程指示您可如何手动调整 iptables。

过程

1. 使用 SSH 作为 root 用户登录到 QRadar。

登录名：<root>

密码：<password>

2. 输入以下命令以编辑 pre 规则 iptables 文件：

   IPv4：

   ```
   vi /opt/qradar/conf/iptables.pre
   ```

   IPv6：

   ```
   vi /opt/qradar/conf/ip6tables.pre
   ```

   将显示 iptables.pre 配置文件。
3. 输入以下命令以编辑 post 规则 iptables 文件：

   IPv4：

   ```
   vi /opt/qradar/conf/iptables.post
   ```

   IPv6：

   ```
   vi /opt/qradar/conf/ip6tables.post
   ```

   将显示 iptables.post 配置文件。
4. 添加以下规则，以便 QRadar 访问特定端口号，其中 *portnumber* 是端口号：

   要接受特定端口输入的 UDP 流量：

   ```
   -A INPUT -m udp -p udp --dport <portnumber> -j ACCEPT
   ```

   要接受特定端口输入的 TCP 流量：

   ```
   -A INPUT -m state --state NEW -m tcp -p tcp --dport <portnumber> -j ACCEPT
   ```
5. 保存 iptables 配置。
6. 运行以下脚本以传播更改：

   ```
   /opt/qradar/bin/iptables_update.pl
   ```
7. 输入以下命令以检查现有 iptables：

   IPv4：

   ```
   iptables -L -n -v
   ```

   IPv6：

   ```
   ip6tables -L -n -v
   ```

数据保留时间

保留存储区可定义在 IBM QRadar 中保留事件和流数据的时间长短。

随着 QRadar 不断接收事件和流，将根据保留存储区过滤条件对每个接收到的事件和流进行比较。当某个事件或流与保留存储区过滤器匹配时，会将其存储在该保留存储区内，直至达到删除策略时间期限为止。缺省保留期为 30 天；那么将立即删除该数据。

保留存储区按优先顺序从顶部行至底部行排序。记录存储在与优先级最高的过滤条件相匹配的存储区内。如果记录不匹配任何已配置的保留存储区，那么此记录会存储在缺省保留存储区内，该存储区始终位于可配置的保留存储区列表下方。

租户数据

您可以为共享数据配置最多 10 个保留存储区，为每个租户配置最多 10 个保留存储区。

数据进入系统时，系统将对数据进行访问，以确定该数据是否为共享数据或者是否属于某个租户。特定于租户的数据将与针对该租户定义的保留存储区过滤器进行比较。当数据匹配保留存储区过滤器时，会将此数据存储在该保留存储区内，直至达到保留策略时间期限为止。

如果您没有为租户配置保留存储区，那么数据将自动放置在该租户的缺省保留存储区。除非您配置特定于租户的保留存储区，否则缺省保留期为 30 天。

配置保留存储区

配置保留时间策略以定义需要 IBM QRadar 将事件和流数据保留的时间长度，以及在数据达到特定时效时需要执行的操作。

关于此任务

对保留存储区过滤器的更改仅立即应用到入局数据。例如，如果配置了保留存储区以将来自源 IP 地址 10.0.0.0/8 的所有数据保留 1 天，并且稍后编辑过滤器以保留来自源 IP 192.168.0.1 的数据，那么无法追溯更改。只要更改过滤器，保留存储区就具有 24 小时的 10.0.0.0/8 数据，并且在过滤器更改后收集的所有数据都是 192.168.0.1 数据。

无论过滤器条件如何，存储区上的保留时间策略都会应用到存储区中的所有数据。使用先前示例，如果将保留时间策略从 1 天更改为 7 天，那么存储区中的 10.0.0.0/8 数据和 192.168.0.1 数据均保留 7 天。

保留存储区的**分布**以数据保留总量在所有保留存储区中的百分比形式指示保留存储区使用率。分布按每租户进行计算。

过程

1. 在导航菜单（☰）上，单击**管理**。
2. 在**数据源**部分中，单击**事件保留时间**或**流保留时间**。
3. 如果配置了租户，请在**租户**列表中，选择要将保留存储区应用到的租户。

   注: 要管理多租户配置中的共享数据的保留时间策略，请在**租户**列表中选择**不适用**。
4. 要配置新保留存储区，请完成下列步骤:
   a) 双击表中的第一个空行以打开“**保留属性**”窗口。
   b) 配置保留存储区参数。

   了解有关保留存储区参数的更多信息:

属性	描述
名称	输入保留存储区的唯一名称。
此存储区中放置的数据的保留时间	用于指定要将数据保留的时间长度的保留期。当达到保留期时，将会根据**删除此存储区中的数据**参数来删除数据。QRadar 不会删除保留期内的数据。
删除此存储区中的数据	选择**在保留期到期后立即删除**以在与**此存储区中放置的数据的保留时间**参数匹配时立即删除数据。无论磁盘存储需求如何，都会在下一个调度的磁盘维护过程中删除数据。 选择**需要存储空间时**以将与**此存储区中放置的数据的保留时间**参数匹配的数据保留在存储器中，直至磁盘监视系统检测到需要存储空间为止。 基于存储空间的删除在可用磁盘空间降至 15% 或更低时开始，并且删除会继续直至可用磁盘空间为 18%，或者**此存储区中放置的数据的保留时间**字段中设置的策略时间范围到期为止。例如，如果记录的已用磁盘空间达到 85%，那么会删除数据，直至已用百分比降至 82% 为止。当需要存储空间时，仅会删除与**此存储区中放置的数据的保留时间**字段匹配的数据。 如果存储区设置为**删除此存储区中的数据：在保留期到期时立即删除**，那么不会执行任何磁盘空间检查，并且删除任务会立即移除超过保留时间的所有数据。
描述	输入保留存储区的描述。
当前过滤器	配置要与每个数据段进行比较的过滤器条件。

   c) 指定每个过滤器条件集后，单击**添加过滤器**。

d) 单击**保存**。

5. 要编辑现有保留存储区，请从表中选择行，然后单击**编辑**。
6. 要删除保留存储区，请从表中选择行，然后单击**删除**。
7. 单击**保存**。

与保留时间策略属性匹配的入局数据立即存储在保留存储区中。

管理保留存储区序列

您可以更改保留存储区的顺序，以确保数据按照匹配需求的顺序匹配保留存储区。

关于此任务

保留存储区在“**事件保留**”和“**流保留**”窗口上按从优先级顺序从第一行到最后一行列出。记录存储在第一个与记录参数匹配的保留存储区中。

无法移动缺省保留存储区。它始终位于列表底部。

过程

1. 在导航菜单（☰）上，单击**管理**。
2. 在**数据源**部分中，单击**事件保留**或**流保留**。
3. 如果已配置租户，请在**租户**列表中，选择要重新排序的保留存储区的租户。

   注: 要在多租户配置中管理共享数据的保留策略，请在**租户**列表中选择 **N/A**。
4. 选择与要移动的保留存储区对应的行，并单击**向上**或**向下**以将其移动到正确位置。
5. 单击**保存**。

启用和禁用保留存储区

配置和保存保留存储区时，缺省情况下会启用保留存储区。您可以禁用存储区以调整事件或流保留。

关于此任务

禁用存储区时，会将与已禁用存储区的需求匹配的任何新事件或流存储在与事件或流属性匹配的新存储区中。

过程

1. 在导航菜单（☰）上，单击**管理**。
2. 在**数据源**部分中，单击**事件保留**或**流保留**。
3. 如果已配置租户，请在**租户**列表中，选择要更改的保留存储区的租户。

   注: 要在多租户配置中管理共享数据的保留策略，请在**租户**列表中选择 **N/A**。
4. 选择要禁用的保留存储区，然后单击**启用/禁用**。

删除保留存储区

删除保留存储区时，仅删除定义此存储区的条件。 存储在此存储区中的事件或流由缺省保留存储区收集。缺省保留期为 30 天；那么将立即删除该数据。

过程

1. 在导航菜单（☰）上，单击**管理**。
2. 在**数据源**部分中，单击**事件保留时间**或**流保留时间**。
3. 如果已配置租户，请在**租户**列表中，选择要删除的保留存储区的租户。

   注: 要管理多租户配置中的共享数据的保留时间策略，请在**租户**列表中选择**不适用**。
4. 选择要删除的保留存储区，然后单击**删除**。

系统通知

IBM QRadar 持续不断地监控所有设备并向 QRadar Console 传递参考、警告和错误通知，让您更轻松地监视部署的状态和运行状况。

要在屏幕上显示系统通知，您必须将自己的浏览器配置为允许弹出窗口，并确保在用户首选项 () 中已选中**启用弹出通知**复选框。如果您禁用了 QRadar 的桌面通知，那么仍可以在通知 () 菜单下查看系统通知。

注: Mozilla Firefox、Google Chrome 和 Microsoft Edge 10 支持浏览器通知。Microsoft Internet Explorer 不支持基于浏览器的通知。Internet Explorer 中的通知显示在 QRadar 通知框中。通知显示的方式以及消息停留在屏幕上的时间可能因浏览器而异。

配置系统通知

您可以配置系统性能警报的阈值。

关于此任务

下表描述了“全局系统通知”窗口参数

表 7. “全局系统通知”窗口参数

参数	描述
1 分钟内的系统负载	输入过去 1 分钟内的平均系统负载阈值。
5 分钟内的系统负载	输入过去 5 分钟内的平均系统负载阈值。
15 分钟内的系统负载	输入过去 15 分钟内的平均系统负载阈值。
设备用于 I/O 请求的平均时间（毫秒）	输入用于 I/O 请求的时间阈值（毫秒）
已用交换空间百分比	输入已用交换空间的百分比阈值。
每秒接收的数据包数	输入每秒接收的数据包数的阈值。
每秒传输的数据包数	输入每秒传输的数据包数的阈值。
每秒接收的字节数	输入每秒接收的字节数的阈值。
每秒传输的字节数	输入每秒传输的字节数的阈值。
接收错误数	输入每秒接收的损坏数据包数的阈值。
传输错误数	输入每秒传输的损坏数据包数的阈值。
数据包冲突数	输入传输数据包时每秒出现的冲突数的阈值。
丢弃的接收数据包数	输入由于缓冲区空间不足，每秒丢弃的已接收数据包数的阈值。
丢弃的传输数据包数	输入由于缓冲区空间不足，每秒丢弃的已传输数据包数的阈值。
传输载波错误数	输入传输数据包时每秒出现的载波错误数的阈值。
接收帧错误数	输入已接收数据包每秒出现的帧定位错误数的阈值。
接收 fifo 过速次数	输入已接收数据包每秒出现的先进先出 (FIFO) 过速错误数的阈值。
传输 fifo 过速次数	输入已传输数据包每秒出现的先进先出 (FIFO) 过速错误数的阈值。

过程

1. 在导航菜单（☰）上，单击**管理**。
2. 在**系统配置**部分中，单击**全局系统通知**。
3. 输入要配置的每个参数的值。
4. 对于每个参数，请选择**已启用**和**响应条件**，然后选择下列其中一个选项：

选项	描述
大于	如果参数值超过配置的值，那么将生成警报。
小于	如果参数值小于配置的值，那么将生成警报。

5. 输入对警报的首选解决方案的描述。
6. 单击**保存**。
7. 在**管理**选项卡上，单击**部署更改**。

配置事件和流定制电子邮件通知

在 IBM QRadar 中配置规则时，指定每次规则生成响应时，就会向收件人发送电子邮件通知。电子邮件通知提供有用的信息，例如事件或流属性。

关于此任务

您可以通过编辑 `alert-config.xml` 文件来定制规则响应的电子邮件通知中包含的内容。

注: 对流的引用不适用于 IBM QRadar Log Manager。

必须创建可以安全编辑文件副本的临时目录，而不会产生覆盖缺省文件的风险。编辑并保存 `alert-config.xml` 文件后，必须运行用于验证更改的脚本。验证脚本自动将更改应用于登台区域。您必须部署完全配置以重新构建所有设备的配置文件。

对于 IBM QRadar on Cloud，您必须开具具有 IBM 支持的凭证以获取 `alert-config.xml` 文件的副本。您必须开具另一个凭证以将更新的 `alert-config.xml` 文件应用于 QRadar on Cloud 实例。

过程

1. 使用 SSH，以 root 用户身份登录 QRadar Console。
2. 创建要用于安全编辑缺省文件副本的新临时目录。
3. 要将 `custom_alerts` 目录中存储的文件复制到临时目录，请输入以下命令：

```
cp /store/configservices/staging/globalconfig/templates/custom_alerts/*.* <directory_name>
```

   <directory_name> 是您创建的临时目录的名称。
4. 确认是否已成功复制文件：
   a) 要列出目录中的文件，请输入 `ls -lah`。
   b) 验证是否列出了 `alert-config.xml` 文件。
5. 打开 `alert-config.xml` 文件进行编辑。
6. 编辑 `<template>` 元素的内容。
   a) 必需： 指定要使用的模板的类型。有效选项为 `event` 或 `flow`。

```
<templatetype>event</templatetype>
```

```
<templatetype>flow</templatetype>
```

   b) 输入电子邮件模板的名称：

```
<templatename>Default flow template</templatename>
```

   如果有多个模板，请确保此模板名称是唯一的。

c) 将 <active> 元素设置为 true：

```
<active>true</active>
```

d) 编辑 <body> 或 <subject> 元素中的参数以包含要查看的信息。

要点： 对于要在 QRadar 中显示为选项的每个事件和流模板类型，必须将 <active></active> 属性设置为 True。每个类型必须有至少一个活动模板。

您还必须确保 <filename></filename> 属性保留为空。

可在模板中使用的通知参数：

表 *8.* 接受的通知参数

公共参数	**事件参数**	**流参数**
AppName	EventCollectorID	Type
RuleName	DeviceId	CompoundAppID
RuleDescription	DeviceName	FlowSourceIDs
EventName	DeviceTime	SourceASNList
EventDescription	DstPostNATPort	DestinationASNList
EventProcessorId	SrcPostNATPort	InputIFIndexList
Qid	DstMACAddress	OutputIFIndexList
Category	DstPostNATIPAddress	AppId
RemoteDestinationIP	DstPreNATIPAddress	Host
有效内容	SrcMACAddress	Port
可信性	SrcPostNATIPAddress	SourceBytes
相关性	SrcPreNATIPAddress	SourcePackets
来源	SrcPreNATPor	Direction
SourcePort	DstPreNATPort	SourceTOS
SourceIP		SourceDSCP
Destination		SourcePrecedence
DestinationPort		DestinationTOS
DestinationIP		DestinationDSCP
DestinationUserName		SourceASN
协议		DestinationASN
StartTime		InputIFIndex
持续时间		OutputIFIndex
StopTime		FirstPacketTime
EventCount		LastPacketTime
SourceV6		TotalSourceBytes
DestinationV6		TotalDestinationBytes
UserName		TotalSourcePackets
DestinationNetwork		TotalDestinationPackets

表 8. 接受的通知参数 (续)		
公共参数	**事件参数**	**流参数**
SourceNetwork		SourceQOS
严重性		DestinationQOS
CustomProperty		SourcePayload
CustomPropertiesList		
CalculatedProperty		
CalculatedPropertiesList		
AQLCustomProperty		
AqlCustomPropertiesList		
LogSourceId		
LogSourceName		

注: 如果您不希望在使用 CustomProperties、CalculatedProperties 或 AqlCustomProperties 参数时检索整个列表，那么可以通过使用以下标记来选择特定属性:

- 定制属性: `${body.CustomProperty("<custom_property_name>")}`
- 计算的属性: `${body.CalculatedProperty("<calculated_property_name>")}`
- AQL 定制属性: `${body.AqlCustomProperty("<AQL_custom_property_name>")}`

7. 要创建多个电子邮件模板，请将 `<template>` 元素中的以下样本电子邮件模板复制并粘贴在 `alert-config.xml` 文件中。针对添加的每个模板重复步骤 6。

样本电子邮件模板:

```
<template>
  <templatename>Default Flow</templatename>
  <templatetype>flow</templatetype>
  <active>true</active>
  <filename></filename>
  <subject>${RuleName} Fired </subject>
  <body>
     The ${AppName} event custom rule engine sent an automated response:

     ${StartTime}

     Rule Name:                                    ${RuleName}
     Rule Description:                             ${RuleDescription}

     Source IP:                                    ${SourceIP}
     Source Port:                                  ${SourcePort}
     Source Username (from event):                 ${UserName}
     Source Network:                               ${SourceNetwork}

     Destination IP:                               ${DestinationIP}
     Destination Port:                             ${DestinationPort}
     Destination Username (from Asset Identity): ${DestinationUserName}
     Destination Network:                          ${DestinationNetwork}

     Protocol:                                     ${Protocol}
     QID:                                          ${Qid}

     Event Name:                                   ${EventName}
     Event Description:                            ${EventDescription}
     Category:                                     ${Category}

     Log Source ID:                                ${LogSourceId}
     Log Source Name:                              ${LogSourceName}

     Payload:                                      ${Payload}

     CustomPropertiesList:                         ${CustomPropertiesList}
```

```
      AQL Custom Property, CEP_aql_1:              ${body.AqlCustomProperty("CEP_aql_1")}

      Calculated Property, CEP_calc_2:             ${body.CalculatedProperty("CEP_calc_2")}

      Regex Property, CEP_reg_3:                   ${body.CustomProperty("CEP_reg_3")}

    </body>
    <from></from>
    <to></to>
    <cc></cc>
    <bcc></bcc>
</template>
```

注: 目前，多租户或重叠的 IP 地址的**域标识**在定制电子邮件模板中不可用。

8. 保存并关闭 `alert-config.xml` 文件。
9. 通过输入以下命令来验证更改。

```
/opt/qradar/bin/runCustAlertValidator.sh <directory_name>
```

<directory_name> 参数是已创建的临时目录的名称。

如果脚本成功验证更改，那么会显示以下消息：`File alert-config.xml was deployed successfully to staging!`

10. 在 QRadar 中部署更改。
    a) 登录 QRadar。
    b) 在导航菜单（☰）上，单击**管理**。
    c) 单击**高级 > 部署完整配置**。

    注: QRadar 在您部署完整配置时会继续收集事件。事件收集服务必须重新启动的情况下，QRadar 并不会将其自动重新启动。将显示一条消息，为您提供选项以取消部署并在更方便的时候重新启动服务。

配置定制攻击电子邮件通知

您可以为针对攻击触发的电子邮件通知创建模板。

您可以通过编辑 `alert-config.xml` 文件来定制电子邮件通知中包含的内容。

必须创建可以安全编辑文件副本的临时目录，而不会产生覆盖缺省文件的风险。编辑并保存 `alert-config.xml` 文件后，必须运行用于验证更改的脚本。验证脚本自动将更改应用于登台区域。您必须部署完全配置以重新构建所有设备的配置文件。

过程

1. 使用 SSH，以 root 用户身份登录 QRadar Console。
2. 创建要用于安全编辑缺省文件副本的新临时目录。
3. 输入以下命令来将 `custom_alerts` 目录中存储的文件复制到临时目录：

```
cp /store/configservices/staging/globalconfig/templates/custom_alerts/*.* <directory_name>
```

<directory_name> 是您创建的临时目录的名称。

如果此文件不存在于 `staging` 目录中，您可能会在 `/opt/qradar/conf/templates/custom_alerts` 目录中找到此文件。

4. 确认是否已成功复制文件：
   a) 要列出目录中的文件，请输入 `ls -lah`。
   b) 验证是否列出了 `alert-config.xml` 文件。
5. 打开 `alert-config.xml` 文件进行编辑。
6. 为新攻击模板添加新的 `<template>` 元素。
   a) 必需： 为模板类型值输入 `offense`。

```
<templatetype>offense</templatetype>
```

b) 输入攻击模板的名称。
例如，<templatename>Default offense template</templatename>

如果有多个模板，请确保此模板名称是唯一的。

c) 将 <active> 元素设置为 true。

```
<active>true</active>
```

要点: 对于要在 QRadar 中显示为选项的每个模板类型，必须将 <active></active> 属性设置为 true。每个类型必须有至少一个活动模板。

d) 编辑 <body> 或 <subject> 元素中的参数以包含要查看的信息。

以下列表提供可在攻击模板中使用的值。$Label 值提供项目的标签，$Value 值提供数据。

攻击参数

$Value.DefaultSubject
$Value.Intro
$Value.OffenseId
$Value.OffenseStartTime
$Value.OffenseUrl
$Value.OffenseMRSC
$Value.OffenseDescription
$Value.EventCounts

$Label.OffenseSourceSummary
$Value.OffenseSourceSummary

$Label.TopSourceIPs
$Value.TopSourceIPs

$Label.TopDestinationIPs
$Value.TopDestinationIPs

$Label.TopLogSources
$Value.TopLogSources

$Label.TopUsers
$Value.TopUsers

$Label.TopCategories
$Value.TopCategories

$Label.TopAnnotations
$Value.TopAnnotations

$Label.ContributingCreRules

$Value.ContributingCreRules

您还可以通过在模板中使用以下语法来对一些值进行循环：

```
#foreach( $item in $Value.X )
  $item
#end
```

其中，*X* 是以下某个值：

- OffenseSourceSummaryList
- TopSourceIPsList
- TopDestinationIPsList
- TopLogSourcesList
- TopUsersList
- TopCategoriesList
- TopAnnotationsList
- ContributingCreRulesList

您可以使用 ${*X*} 来包含以下属性，其中 *X* 是以下某个值：

- OffenseID
- OffenseRuleID
- OffenseRuleName
- Magnitude
- Relevance
- Severity
- Credibility
- Domain（如果找不到，则为“N/A”）
- Tenant（如果找不到，则为“N/A”）
- OffenseType

例如，如果攻击的规模为 7，并且在模板中包含 ${Magnitude}，那么在电子邮件中 ${Magnitude} 的值显示为 7。

7. 保存并关闭 alert-config.xml 文件。
8. 通过输入以下命令来验证更改。

```
/opt/qradar/bin/runCustAlertValidator.sh <directory_name>
```

<directory_name> 是您创建的临时目录的名称。

如果脚本成功验证更改，那么会显示以下消息：File alert-config.xml was deployed successfully to staging!

9. 在 QRadar 中部署更改。
   a) 登录 QRadar。
   b) 在导航菜单（☰）上，单击**管理**。
   c) 单击**高级** > **部署完整配置**。

   注： QRadar 在您部署完整配置时会继续收集事件。事件收集服务必须重新启动的情况下，QRadar 并不会将其自动重新启动。将显示一条消息，为您提供选项以取消部署并在更方便的时候重新启动服务。

定制攻击关闭原因

您可管理**攻击**选项卡上的**关闭原因**列表框中列出的选项。

当用户关闭**攻击**选项卡上的攻击时，会显示“关闭攻击”窗口。系统会提示用户从**关闭原因**列表框中选择原因。其中列出了三个缺省选项：

- 误判，已调整
- 不属于问题
- 策略违例

管理员可以从**管理员**选项卡添加、编辑和删除定制攻击关闭原因。

添加定制攻击关闭原因

添加定制攻击关闭原因时，新原因会列示在“**定制关闭原因**”窗口上，以及“**关闭攻击**”窗口上**攻击**选项卡的**关闭原因**列表框中。

过程

1. 在导航菜单（☰）上，单击**管理**。
2. 在**系统配置**部分中，单击**定制攻击关闭原因**。
3. 单击**添加**。
4. 输入唯一的攻击关闭原因。原因长度必须介于 5 与 60 个字符之间。
5. 单击**确定**。

   新的定制攻击关闭原因现在会在“**定制关闭原因**”窗口中列出。“**关闭攻击**”窗口上**攻击**选项卡的**关闭原因**列表框还会显示您添加的定制原因。

编辑定制攻击关闭原因

编辑定制攻击关闭原因，会从“**定制关闭原因**”窗口和**攻击**选项卡的“**关闭攻击**”窗口上的**关闭原因**列表框中更新原因。

过程

1. 在导航菜单（☰）上，单击**管理**。
2. 在**系统配置**部分中，单击**定制攻击关闭原因**。
3. 选择要编辑的攻击关闭原因。
4. 单击**编辑**。
5. 输入关闭攻击的新的唯一原因。原因长度必须为 5 到 60 个字符。
6. 单击**确定**。

删除定制攻击关闭原因

删除定制攻击关闭原因，会从“**定制关闭原因**”窗口和**攻击**选项卡上“**关闭攻击**”窗口上的**关闭原因**列表框中移除原因。

过程

1. 在导航菜单（☰）上，单击**管理**。
2. 在**系统配置**部分中，单击**定制攻击关闭原因**。
3. 选择要删除的攻击关闭原因。
4. 单击**删除**。
5. 单击**确定**。

配置定制的资产属性

针对 IBM QRadar 中的资产运行查询时，定制资产属性可提供更多查询选项。

过程

1. 在导航菜单（☰）上，单击**管理**。
2. 在**系统配置**部分中，单击**定制资产属性**。
3. 在**名称**字段中，输入该定制资产属性的描述符。

   注: 该名称只能包含字母数字字符、空格和下划线。不允许使用特殊字符。
4. 在**类型**列表中，选择**数字**或**文本**，以定义该定制资产属性的信息类型。
5. 单击**确定**。
6. 单击**资产**选项卡。
7. 单击**编辑资产 > 定制资产属性**。
8. 在值字段中输入必需的信息。
9. 单击**确定**。

添加定制操作

将脚本附加到定制规则以执行特定操作来响应网络事件。使用“**定制操作**”窗口以管理定制操作脚本。

使用定制操作来选择或定义传递到脚本和生成的操作的值。

例如，您可以编写脚本以创建防火墙规则，阻止网络中的源 IP 地址响应定义的尝试登录失败次数所触发的规则。

以下示例是作为将值传递到脚本的结果的定制操作:

· 阻止用户和域。

· 启动外部系统中的工作流和更新。

· 使用线程的 STIX 表示更新 TAXI 服务器。

定制操作最适合少量定制规则事件和响应限制器值较低的定制规则。

1. 在导航菜单（☰）上，单击**管理**。
2. 在**定制操作**部分中，单击**定义操作**。
3. 要更新脚本，请单击**添加**。将在**解释器**列表中列出产品支持的编程语言版本。

   出于部署的安全性考量，QRadar 不支持随 Python、Perl 或 Bash 语言提供的全部脚本编制功能。
4. 指定要传递给已上载的脚本的参数。

表 *9.* 定制操作参数

参数	**描述**
固定属性	传递给定制操作脚本的值。 这些属性并非基于事件或流本身，而是涵盖您可以使用脚本来处理的其他已定义值。例如，将第三方系统的固定属性 **username** 和 **password** 传递到用于发送 SMS 警报的脚本。 选中**对值进行加密**复选框以对固定属性进行加密。

表 9. 定制操作参数 (续)	
参数	**描述**
网络事件属性	由事件生成的动态 Ariel 属性。可从**属性**列表中选择。 例如，网络事件属性 **sourceip** 提供匹配触发的事件的源 IP 地址的参数。 有关 Ariel 属性的更多信息，请参阅 *IBM QRadar Ariel Query Language Guide*。

参数按添加到“**定制操作**”窗口中的顺序传递到脚本。

运行定制操作脚本时，会在 /opt/qradar/bin/ca_jail/ 目录中设置 chroot jail。/opt/qradar/bin/ca_jail/ 目录中的任何内容均可由脚本进行修改和写入脚本。定制操作用户主目录 (/home/customactionuser) 同样可修改。

脚本只能从 jail 环境内部运行，这样就不会影响 QRadar 运行环境。定制操作执行期间的所有文件访问都与 /opt/qradar/bin/ca_jail/ 目录相关。

定制操作用户帐户可能无权运行后续命令，例如，登录防火墙和阻止 IP 地址。请先测试脚本是否可成功运行，然后再将其与规则关联。

注: 您要实施的定制操作的类型取决于您的网络基础结构及其组件。例如，您可以在 Cisco 设备上配置 REST API 以阻止可疑 IP 地址。其他第三方供应商可能不提供 REST 接口，因此您可能需要开发自己的 Web Service 解决方案以运行定制操作。

您必须在源自 Windows 或 DOS 系统的脚本上运行 dos2unix 实用程序。Windows 或 DOS 系统通常会添加控制字符。要在 QRadar 中使用**测试执行**功能来成功测试定制操作脚本，必须移除控制字符。

相关信息

定制操作脚本简介

测试定制操作

请先测试您的脚本是否成功运行并有预期的结果，再将它与规则相关联。

关于此任务

定制操作脚本在与生产环境隔离的测试环境中运行。一般而言，定制操作脚本在运行事件处理器的受管主机上运行。但是，如果您是使用“一体化”设备，那么定制操作是在 QRadar Console 上运行。

测试执行仅在 QRadar Console 上受支持，在受管主机上不受支持。

如果必须从定制操作脚本写入磁盘，那么您必须使用下列目录：/home/customactionuser。

过程

1. 在导航菜单（☰）上，单击**管理**。
2. 在**定制操作**部分中，单击**定义操作**。
3. 从列表中选择定制操作，并单击**测试执行** > **执行**以测试您的脚本。测试结果以及该脚本所产生的任何输出随即返回。
4. 在配置和测试定制操作后，使用**规则向导**以创建新事件规则并将定制操作与其相关联。

   有关事件规则的更多信息，请参阅《*IBM QRadar User Guide*》。

将参数传递到定制操作脚本

Bash、Python 和 Perl 中的样本脚本显示了如何将参数传递到定制操作脚本。

以下简单样本脚本显示了如何使用提供的攻击源 IP 地址来查询资产的资产模型 API。为了此示例的需要，脚本会输出端点返回的 JSON。

该脚本需要三个参数:

· Console IP 地址

· API 令牌

· 攻击源 IP 地址

这些参数是在“定义定制操作”窗口的**脚本参数**区域中配置的：

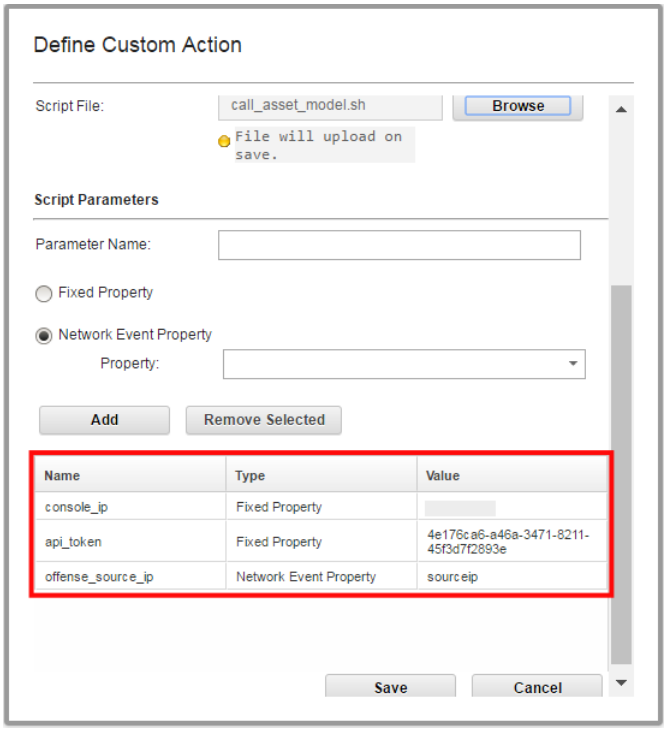

图 *5.* 定制操作脚本参数

每个参数都会按“定义定制操作”窗口中添加这些参数的顺序传递到脚本。在此案例中顺序为：

1. console_ip
2. api_token
3. offense_source_ip

在每个样本脚本开头处定义的变量使用“定义定制操作”窗口中添加的样本参数名称：

```
#!/bin/bash
console_ip=$1
api_token=$2
offense_source_ip=$3

auth_header="SEC:$api_token"

output=$(curl -k -H $auth_header https://$console_ip/console/restapi/api/
asset_model/assets?filter=interfaces%20contains%20%28%20ip_addresses
%20contains%20%28%20value%20%3D%20%22$offense_source_ip%22%29%29)

# Basic print out of the output of the command
echo $output
```

图 *6. call_asset_model.sh*

```
#!/usr/bin/python
import sys
import requests
console_ip = sys.argv[1]
api_token = sys.argv[2]
offense_source_ip = sys.argv[3]

auth_header = {'SEC' : api_token }

endpoint = "https://{0}/console/restapi/api/asset_model/
assets?filter=interfaces%20contains%20%28%20ip_addresses
%20contains%20%28%20value%20%3D%20%22{1}%22%29%29"
.format(console_ip, offense_source_ip)

response = requests.get(endpoint, headers=auth_header, verify=False)

# Basic print out of the output of the command
print(response.json())
```

图 *7. call_asset_model.py*

```
#!/usr/bin/perl
use strict;
use warnings;
use LWP::UserAgent;

my $console_ip = $ARGV[0];
my $api_token = $ARGV[1];
my $offense_source_ip = $ARGV[2];

my $endpoint = "https://$console_ip/console/restapi/api/asset_model/
assets?filter=interfaces%20contains%20%28%20ip_addresses
%20contains%20%28%20value%20%3D%20%22$offense_source_ip%22%29%29";

my $client = LWP::UserAgent -> new(ssl_opts => { verify_hostname => 0 });

my $response = $client -> get($endpoint, "SEC" => $api_token);

# Basic print out of the output of the command
print $response -> decoded_content;
```

图 *8. call_asset_model.pl*

管理汇总数据视图

大量数据汇总会降低系统性能。Ariel 函数将单独数据库用于汇总数据，以便提高系统性能以及更易于访问数据。您可以禁用、启用或删除汇总数据视图。时间序列图、报告图表和异常规则使用汇总数据视图。

关于此任务

在**显示**列表中显示的项将对数据排序。

“汇总数据视图”需要生成 ADE 规则、时间序列图表和报告的数据。

如果达到最大视图数，禁用或删除视图。

可能会在**汇总数据标识**列中出现重复视图，因为汇总数据视图可包含多个搜索。

过程

1. 在导航菜单（☰）上，单击**管理**。
2. 在**系统配置**部分中，单击**聚合数据管理**。
3. 对汇总数据视图的列表进行过滤，请执行以下其中一个选项：
   - 从**视图**、**数据库**、**显示 (Show)** 或**显示 (Display)** 列表中选择一个选项。
   - 在搜索字段中输入汇总数据标识、报告名称、图表名称或已保存搜索名称。
4. 要管理汇总数据视图，请选择视图，然后在工具栏上单击相应操作：

- 如果选择**禁用视图**或**删除视图**，那么会显示汇总数据视图的内容依赖关系。禁用或删除视图后，依赖的组件不再使用汇总数据。
- 启用先前禁用的汇总数据视图以复原视图。

表 *10.* 汇总数据管理视图的列描述

列	**描述**
汇总数据标识	汇总数据的标识
已保存的搜索名称	已保存的搜索的定义名称
列名	列标识
时间搜索	搜索计数
写入的数据	已写入数据的大小
数据库名称	写入文件的数据库
上次修改时间	最后一次修改数据的时间戳记
已启用唯一计数	True 或 False：搜索结果以显示唯一事件和流计数而不是一段时间的平均计数。

第 6 章 在 QRadar 中处理事件数据

在 IBM QRadar 中，使用 DSM Editor 解决解析问题及添加定制解析。

DSM Editor 提供实时反馈，以便了解定制按预期方式工作。

相关概念
IBM QRadar 产品中的功能

DSM 编辑器概述

可以使用 DSM 编辑器代替手动创建日志源扩展来修复分析问题或扩展对新日志源类型的支持。DSM 编辑器为您的数据提供了不同的视图。使用 DSM 编辑器以抽取字段、定义定制属性、分类事件以及定义新的 QID 定义。

DSM 编辑器提供以下视图：

工作空间

工作空间向您显示原始事件数据。使用样本事件有效内容来测试日志源类型的行为，然后**工作空间**区域向您显示实时捕获的数据。

所有样本事件都会从工作空间发送到在其中解析属性并查找 QID 映射的 DSM 模拟器。在**日志活动预览**部分中显示结果。单击编辑图标可以在编辑方式下打开。

在编辑方式中，最多可以将 100,000 个字符的事件数据粘贴到工作空间或者直接编辑数据。在**属性**选项卡上编辑属性时，将在工作空间中突出显示有效内容中的匹配。还将在**工作空间**中突出显示定制属性和覆盖的系统属性。

日志活动预览

日志活动预览模拟工作空间中的有效内容在**日志活动**查看器中的显示方式。将显示每个受支持的标准属性。将从 QID 映射填充标记星号 (*) 的字段，例如，**事件名称**、**严重性**、**低级别类别**和 **QID**。无法从工作空间中的原始事件，逐字解析从 QID 映射填充的字段，因此无法定义或进行编辑。您可以通过从**事件映射**选项卡中选择对应的事件标识和类别组合，调整它们的值。然后，单击**编辑**以将事件重新映射到系统中已有的其他 QID 记录或新创建的 QID。

单击配置图标以选择要在**日志活动预览**窗口中显示或隐藏的列，然后对列进行重新排序。

属性

属性选项卡包含系统和定制属性（构成 DSM 配置）的组合集。配置系统属性不同于配置定制属性。您可以通过选择**覆盖系统行为**复选框并定义表达式来覆盖属性。

注: 如果覆盖**事件类别**属性，那么您还必须覆盖**事件标识**属性。

有效内容中的匹配项将突出显示在工作空间中的事件数据内。突出显示的颜色有两种色调，具体取决于您捕获的内容。例如，以橙色突出显示的内容表示捕获组值，而亮黄色突出显示的内容表示您指定的正则表达式的其余部分。工作空间中的反馈显示是否有正确的正则表达式。如果某个表达式处于焦点中，那么工作空间中突出显示的内容将仅反映该表达式可以匹配的内容。如果整个属性都处于焦点中，那么突出显示的内容将变为绿色并显示这组汇总表达式可以匹配的内容，并同时考虑优先顺序。

在**格式字符串**字段中，捕获组使用 *$<number>* 表示法表示。例如，$1 表示正则表达式中的第一个捕获组，而 $2 是第二个捕获组，依此类推。

您可以向同一属性中添加多个表达式，并且可以通过将表达式拖放到列表顶部来指定优先顺序。

任何属性旁边的警告图标指示未添加任何表达式。

事件映射选项卡

事件映射选项卡显示系统中针对选中的日志源类型存在的所有事件标识和类别组合。如果创建新事件映射，那么会将其添加到在**事件映射**选项卡中显示的事件标识和类别组合列表。通常，**事件映射**选项卡显示所有事件标识和类别组合以及将它们映射到的 QID 记录。

“配置”选项卡

您可以针对 JSON 格式的结构化数据配置“自动属性发现”。缺省情况下，日志源类型已关闭“自动属性发现”。

在**配置**选项卡上启用**自动属性发现**时，属性发现引擎自动生成新属性以捕获日志源类型收到的事件中存在的所有字段。您可以在**发现完成阈值**字段中配置要针对新属性检查的连续性事件的数量。新发现的属性在**属性**选项卡中显示，并且可用于规则和搜索索引。但是，如果在阈值之前未发现新属性，那么发现过程视为完成并且禁用此日志源类型的**自动属性发现**。您可以随时在“配置”选项卡上手动启用“自动属性发现”。

注: 要持续检查某种日志源类型的事件，必须确保将**发现完成阈值**值设置为 0。

相关概念

DSM 编辑器中的属性
在 DSM 编辑器中，规范化的属性将与定制属性进行组合并按字母顺序进行排序。

DSM 编辑器中的属性

在 DSM 编辑器中，规范化的属性将与定制属性进行组合并按字母顺序进行排序。

DSM 不能具有多个同名属性。

系统属性的配置与定制属性不同。

系统属性

系统属性无法删除，但是可覆盖缺省行为。有两种类型的系统属性：

预定义的系统属性

显示用于 DSM 的缺省 QRadar 行为。

覆盖系统属性

配置了覆盖（日志源扩展）的系统属性在状态行中显示**覆盖**。系统属性具有覆盖时，此 DSM 的日志源扩展使用针对配置输入的正则表达式。

定制属性

定制属性在状态行中显示**定制**。

定制属性在以下方面与系统属性不同：

- 定制属性在其名称下显示**定制**。
- 定制属性无**覆盖系统行为**复选框。
- 要使定制属性可用于规则和搜索索引，请在创建定制属性时选择**启用此属性以用于规则和搜索索引**复选框。

  注: 选择此选项时，QRadar 尝试在事件进入管道后立即从事件抽取属性。将持久存储抽取的属性信息和事件记录的其余部分。在用于搜索或报告时，无需再次抽取属性。该过程可增强检索属性时的性能，但是在事件收集和存储期间，此过程可能对性能造成负面影响。
- 定制属性必须具有一个或多个表达式才有效。

相关概念

DSM 编辑器概述

可以使用 DSM 编辑器代替手动创建日志源扩展来修复分析问题或扩展对新日志源类型的支持。DSM 编辑器为您的数据提供了不同的视图。使用 DSM 编辑器以抽取字段、定义定制属性、分类事件以及定义新的 QID 定义。

DSM 编辑器中的定制属性定义
您可在单独 DSM 中定义定制属性和复用相同属性。在搜索和规则中使用这些属性，并使用这些属性来允许通过用户定义的特定行为将值解析到这些字段中。

DSM 编辑器中的属性配置

配置 DSM 编辑器中的属性以更改被覆盖的系统属性或 DSM 定制属性的行为。

覆盖系统属性的行为时，必须在“**属性**”选项卡上提供有效的表达式。**格式字符串**字段是正则表达式捕获组和字面值字符的组合。该字符串用于使用从事件捕获的一个或多个值以及其他格式字符或插入信息来填充系统属性。例如，您可能想要解析 IP 地址和端口以将两者组合为一个字符串。如果正则表达式 (regex) 具有两个捕获组，那么可以使用以下格式字符串将二者组合起来：$1:$2。

注意: DSM 编辑器允许在任何特定匹配中引用捕获组 1 - 9。如果引用高于 9 的任何捕获组，那么日志源扩展可能无法正常运行。

您必须配置创建的每个定制属性。您必须在“**属性**”选项卡上为定制属性提供有效的表达式和捕获组。您还可以定义选择性并启用或禁用表达式。

相关概念
第 68 页的『DSM 编辑器中的定制属性定义』
您可在单独 DSM 中定义定制属性和复用相同属性。在搜索和规则中使用这些属性，并使用这些属性来允许通过用户定义的特定行为将值解析到这些字段中。

编写格式字符串以使用捕获字符串

使用**属性配置**选项卡上的**格式字符串**字段以引用在正则表达式中定义的捕获组。按照捕获组的优先顺序引用捕获组。

关于此任务

捕获组是包含在括号中的任意正则表达式。使用 $n 表示法引用捕获组，其中 n 是包含正则表达式 (regex) 的组号。您可以定义多个捕获组。

例如，您具有包含公司和主机名变量的有效内容。

```
"company":"ibm", "hostname":"localhost.com"
"company":"ibm", "hostname":"johndoe.com"
```

您可以使用捕获组来定制来自有效内容的主机名以显示 *ibm.hostname.com*。

过程

1. 在**正则表达式**字段中，输入以下正则表达式：`"company":"(.*?)".*"hostname":"(.*?)"`
2. 在**格式字符串**字段中，输入捕获组 $1.$2，其中 $1 是公司变量的值（在此例中为 ibm），$2 是有效内容中主机名的值。将给出以下输出：

   `ibm.localhost.com ibm.johndoe.com`

针对结构良好的日志编写正则表达式

结构良好的日志是由一组属性组成并且按照以下方式显示的事件格式化样式：

```
<name_of_property_1><assignment_character>
<value_of_property_1><delimiter_character>
<name_of_property_2><assignment_character>
<value_of_property_2><delimiter_character>
<name_of_property_3><assignment_character>
<value_of_property_3><delimiter_character>...
```

使用以下常规准则：

· *<assignment_character>* 可以是“=”或“:”，或者多字符序列，例如“->”。

· *<delimiter_character>* 可以是空格字符（空格键或 Tab 键）或者定界符列表，例如，逗号或分号。

· *<value_of_property>* 和 *<name_of_property>*（某些时候）括在引号或者其他包裹字符中。

例如，考虑设备或应用程序生成的简单登录事件。设备可能报告用户登录的帐户、登录的发生时间以及用户登录所用的计算机的 IP 地址。名称/值对样式事件可能类似于以下片段：

```
<13>Sep 09 22:40:40 192.0.2.12 action=login  accountname=JohnDoe  clientIP=192.0.2.24
timestamp=01/09/2016 22:40:39 UTC
```

注: 字符串“<13>Sep 09 22:40:40 192.0.2.12”是系统日志标题。此字符串不属于事件主体。

下表显示如何捕获结构以上良好的日志示例的属性：

表 *11.* 用于捕获结构良好的日志的属性的正则表达式

属性	**正则表达式**
action	action=(.*?)\t
accountname	accountname=(.*?)\t
clientIP	clientIP=(.*?)\t
timestamp	timestamp=(.*?)\t

方括号中括起的模式表示捕获组。表中的每个正则表达式将捕获等号 (=) 之后且在跳进字符之前的任何内容。

针对自然语言日志编写正则表达式

自然语言日志采用类似于语句的格式，并且每个事件类型可能看起来不同。

例如，简单登录事件可采用以下格式进行表示：

```
<13>Sep 09 22:40:40 192.0.2.12 Account JohnDoe initiated a login action
from 192.0.2.24 at 01/09/2016 22:40:39 UTC
```

下表显示如何捕获以上示例中的自然语言日志的属性：

表 *12.* 用于捕获自然语言日志的属性的正则表达式

属性	**正则表达式**
action	initiated a (.*?) action
accountname	Account (.*?) initiated
clientIP	from (.*?) at
timestamp	at (.*?)

注: 针对自然语言日志编写表达式要求您在创建捕获组之前查看围绕要捕获的值的静态信息。

针对 JSON 格式的结构化数据编写表达式

JSON 格式的结构化数据包含一个或多个属性，表示为键/值对。

关于此任务

您可以通过编写与属性匹配的 JSON 表达式，从以 JSON 格式表示的事件数据抽取属性。JSON 表达式必须是 /"*<name of top-level field>*" 格式的路径。

例如，您拥有采用 JSON 格式化的事件数据：

```
{ "action": "login", "user": "John Doe" }
```

或具有嵌套 JSON 格式的事件，例如：

```
{ "action": "login", "user": { "first_name": "John", "last_name": "Doe" } }
```

过程

要从事件数据抽取属性，请选择以下某种方法：

- 要抽取采用 JSON 格式化的事件数据的“user”属性，请在**表达式**字段中输入表达式 /"user"。
- 对于具有嵌套 JSON 格式的事件，要抽取用户的“last_name”，请在**表达式**字段中输入表达式 /"user"/"last_name"。

编写 JSON 密钥路径表达式

要唯一标识想要从 JSON 对象抽取的字段，JSON 表达式必须遵循特定 JSON 密钥路径约定。

将以下准则用于 JSON 密钥路径表达式：

- 所有 JSON 密钥路径必须以正斜杠 (/) 开头。所有路径必须从根 JSON 对象开始。密钥路径中的后续斜杠指示对 JSON 对象中嵌套的字段的访问权。
- 字段名称必须用双引号括起来。

  有效路径可能类似于以下示例：

  ```
  /"object"/"nestedObject"/"furtherNestedObject"/"desiredPropertyName"
  ```

- 方括号指示 JSON 数组的处理。

  如果未在方括号中提供索引，那么将抽取数组的整个主体。如果在方括号中提供索引，那么将抽取或嵌套数组中的此索引。数组从 0 索引开始，其中 0 是数组中的第一个索引，1 是数组中的第二个索引，如此类推。

  在以下密钥路径示例中，JSON 解析器查看“object”JSON 数组的第二个索引，然后在此数组索引中，查找名为“desiredPropertyName”的字段。

  ```
  /"object"[1]/"desiredPropertyName"
  ```

- 在日志源扩展中，您可以提供和组合多个 JSON 密钥路径以提供单个结果；此约定排除定制属性。您还可以选择包含字面值文本。每个 JSON 密钥路径都必须用花括号括起来。

  请考虑以下示例：

  ```
  {/"object"/"nestedObject"/"desiredPropertyName1"} {/"object"/"nestedObject"/"desiredPropertyName2"}
  ```

  您从第一个 JSON 密钥路径获取解析值，即字面值文本空格，然后从第二个 JSON 密钥路径获取一个解析值。

示例： 以下两个示例显示如何从 JSON 对象抽取数据：

- JSON 对象的简单案例：

  ```
  [{"name":"object1","field1":"value1"}, {"name":"object2","field2":"value2"},
   {"name":"object3","field3":"value3"}]
  ```

  下表显示在此样本对象中可从密钥路径抽取的值：

表 *13.* 来自简单 *JSON* 对象的密钥路径

密钥路径	描述	值
/[]	从 JSON 对象的根抽取整个 JSON 数组。	`[{"name":"object1","field1":"value1"},{"name":"object2","field2":"value2"},{"name":"object3","field3":"value3"}]`
/[1]/"name"	从 JSON 对象的根 JSON 数组中的索引 1 抽取名为“name”的属性的值。	object2

· JSON 对象的复杂案例：

```
<13>May 22 10:15:41 log.test.com {"module":"CPHalo","version":"1.0","user_name":"user123",
"event_type":"File integrity scan request created",
"event_category":"File Integrity Scanning Management","srcName":"domain-lab-123",
"timestamp":"2018-12-02T15:36:17.486","user":
{"email":"user123@example.com","first_name":"fname",
"last_name":"lname","alias":["alias name","alias1","name"]},"client_ip":"12.12.12.12",
"server_id":"12317412471421274","server_reported_fqdn":"None","actor_country":"USA",
"server_group_name":"Example Server","server_platform":"Linux",
"message":"A file integrity monitoring scan was requested for Linux server domain-lab-123
 (13.13.13.13) by Halo user user123@example.com from IP address 12.12.12.12 (USA).",
"type":"fim_scan_request_created","id":"c2e8bf72-b74f-11e2-9055-870a490fcfb6"}
```

下表显示在此样本对象中可从密钥路径抽取的值：

表 *14.* 来自复杂 *JSON* 对象的密钥路径

密钥路径	描述	值
/"user_name"	从 JSON 对象的根抽取“user_name”属性的值。	user123
/"user"/"alias"[]	抽取“user”JSON 对象下嵌套的名为“alias”的整个 JSON 数组。	["alias name","alias1","name"]
/"user"/"alias"[0]	抽取“user”JSON 对象下嵌套的“alias”JSON 数组中索引 0 处的值。	alias name
/"user"/'first_name"	抽取“user”JSON 对象下嵌套的名为“first_name”的属性的值。	fname
{/"user"/"first_name"}.{/"user"/"last_name"}	抽取“user”JSON 对象下嵌套的名为“first_name”的属性的值，然后插入字面值“.”字符，随后抽取“user”JSON 对象下嵌套的名为“second_name”的属性的值。 仅与 DSM 编辑器中的日志源扩展和非定制属性相关。此操作在定制属性中不可行。	fname.lname
{/"user"/"alias"[1]}@{/"client_ip"}	抽取“user”JSON 对象下嵌套的“alias”JSON 数组的索引 1 处的值，插入字面值“@”字符，然后抽取根 JSON 对象下名为“client_ip”的属性的值。 仅与 DSM 编辑器中的日志源扩展和非定制属性相关。此操作在定制属性中不可行。	alias1@12.12.12.12

针对 LEEF 格式的结构化数据编写表达式

LEEF 格式的结构化数据包含一个或多个属性，表示为键/值对。

关于此任务

您可以通过编写匹配属性的 LEEF 表达式，从以 LEEF 格式表示的事件抽取属性。有效 LEEF 表达式采用单个键引用或特殊 LEEF 头字段引用的格式。

例如，您具有采用 LEEF V1.0 格式化的事件，例如：

```
LEEF:1.0|ABC Company|SystemDefender|1.13|console_login|devTimeFormat=yyyy-MM-
dd'T'HH:mm:ss.SSSZ
devTime=2017-10-18T11:26:03.060+0200    usrName=flastname    name=Firstname Lastname
authType=interactivePassword    src=192.168.0.1
```

或者，使用插入标记 (^) 分隔符的 LEEF V2.0 格式化的事件，例如：

```
LEEF:2.0|ABC Company|SystemDefender|1.13|console_login|^|devTimeFormat=yyyy-
MMdd'T'HH:mm:ss.SSSZ^
devTime=2017-10-18T11:26:03.060+0200^usrName=flastname^name=Firstname Lastname
^authType=interactivePassword^src=192.168.0.1
```

过程

通过选择以下某种方法，您可以从事件抽取属性或头键属性：

- 要抽取“usrName”属性，请在 **LEEF 键**字段中输入 `usrName`。

  可抽取的可能的键为：

  - devTimeFormat
  - devTime
  - usrName
  - name
  - authType
  - src
- 要抽取头键属性，请在 **LEEF 键**字段中输入以下格式的键：

  ```
  $eventid$
  ```

  可使用以下表达式抽取 LEEF 头值：

  - $leefversion$
  - $vendor$
  - $product$
  - $version$
  - $eventid$

针对 CEF 格式的结构化数据编写表达式

CEF 格式的结构化数据包含一个或多个属性，表示为键/值对。

关于此任务

您可以通过编写匹配属性的 CEF 表达式，从以 CEF 格式表示的事件抽取属性。有效 CEF 表达式采用单个键引用或特殊 CEF 头字段引用的格式。

例如，您具有采用 CEF 格式化的事件：

```
CEF:0|ABC Company|SystemDefender|1.13|console_login|Console Login|1|start=Oct 18 2017 11:26:03
duser=jsmith cs1=John Smith cs1Label=Person Name cs2=interactivePassword cs2Label=authType
src=1.1.1.1
```

过程

通过选择以下某种方法，您可以从事件抽取属性或头键属性：

- 要抽取“cs1”属性，请在 **CEF 键**字段中输入 cs1。

  可抽取的可能的键为：

  - start
  - duser
  - cs1
  - cs1Label
  - cs2
  - cs2Label
  - src
- 要抽取头键属性，请在 **CEF 键**字段中输入以下格式的键：

  ```
  $id$
  ```

  可使用以下表达式抽取 CEF 头值：

  - $cefversion$
  - $vendor$
  - $product$
  - $version$
  - id
  - $name$
  - $severity$

针对“名称值对”格式的结构化数据编写表达式

“名称值对”格式的结构化数据包含一个或多个属性，表示为键/值对。

关于此任务

您可以通过编写与属性匹配的表达式，从使用“名称值对”格式的事件抽取属性。有效的“名称值对”表达式采用单个键引用的格式。

以下示例显示了使用“名称值对”格式的事件：

```
Company=ABC
Company;Product=SystemDefender;Version=1.13;EventID=console_login;Username=jsmith;Name=John
Smith;authType=interactivePassword;
```

过程

1. 要抽取 Username 属性，请在**表达式**字段中输入 Username。
2. 在**值定界符**字段中，输入有效内容的特定键/值定界符。在此示例中，键/值定界符是等号 (=)。
3. 在**定界符**字段中，在有效内容的特定键/值对之间输入定界符。在此示例中，键/值对之间的定界符是分号 (;)。

结果

有效内容中的匹配项将突出显示在 DSM 编辑器的**工作空间**中的事件数据内。

针对“通用列表”格式的结构化数据编写表达式

“通用列表”格式的结构化数据包含一个或多个属性，表示为列表项。

关于此任务

您可以通过编写与属性匹配的表达式，从使用“通用列表”格式的事件抽取属性。有效的“通用列表”表达式采用 *$<number>* 表示法形式。例如，$0 表示列表中的第一个属性，$1 为第二个属性，以此类推。

以下示例显示了使用“通用列表”格式的事件：

```
ABC Company;1.13;console_login;jsmith;John Smith;interactivePassword;
```

过程

1. 要抽取列表中的第一个属性，请在**表达式**字段中输入 $0。
2. 在**定界符**字段中，在有效内容的特定列表项之间输入定界符。在此示例中，列表项之间的定界符是分号 (;)。

结果

有效内容中的匹配项将突出显示在 DSM 编辑器的**工作空间**中的事件数据内。

打开 DSM 编辑器

您可以从**日志活动**选项卡打开 DSM 编辑器，如果您是管理员，还可以从**管理**选项卡将其打开。例如，如果未正确处理发送到系统的事件，那么可从**日志活动**选项卡选择事件数据，并将其发送到 DSM 编辑器。针对尚未发送到系统的事件，您必须是管理员，从**管理** DSM 选项卡访问 DSM 编辑器。

过程

1. 要从**管理**选项卡打开 DSM 编辑器，请完成下列步骤：
   a) 在导航菜单（☰）上，单击**管理**。
   b) 在**数据源**部分中单击 **DSM 编辑器**。
2. 要从**日志活动**选项卡打开 DSM 编辑器，请完成下列步骤：
   a) 单击**日志活动**选项卡。
   b) 暂停传入的结果，然后突出显示一个或多个事件。

      要点: 如果选择来自两个或更多日志源的多个事件，那么系统会提示您选择要对其操作的日志源类型。您只能选择一种登录源类型，且仅会将日志活动中与所选日志源类型匹配的事件自动添加到工作空间。
   c) 在导航菜单中，选择**操作** > **DSM 编辑器**

配置日志源类型

使用 DSM 编辑器，可在 IBM QRadar 中配置新的日志源类型或使用现有日志源类型。

过程

1. 在导航菜单（☰）上，单击**管理**。
2. 在**数据源**部分中单击 **DSM 编辑器**。
3. 创建日志源类型或选择现有日志源类型：

- 要创建新的日志源类型，并单击**新建**并按照提示操作。
- 要找到现有日志源类型，请使用**过滤器**字段，然后单击**选择**。

为日志源类型配置属性自动检测

启用**属性自动检测**时，会自动生成新的属性，以捕获所选日志源类型接收的事件中存在的所有字段。为日志源类型配置新属性的属性自动检测，这样则不需要为每个实例手动创建一个定制属性。

关于此任务

缺省情况下，日志源类型的**属性自动检测**处于禁用状态。

过程

1. 在 DSM 编辑器中，从“**选择日志源类型**”页面中选择日志源类型或创建新的日志源类型。
2. 单击**配置**选项卡。
3. **限制:** 属性自动检测仅适用于格式为 JSON、CEF、LEEF 或“名称值对”的结构化数据。

   单击**启用属性自动检测**。
4. 从**属性检测格式**列表选择日志源类型的结构化数据格式。

   如果选择**名称值对**，那么在**名称值对中的定界符**部分中，输入用于分隔每个名称和值的定界符，以及用于分隔每个名称值对的定界符。自动创建每对的定界符。
5. 要使新属性可用于规则和搜索，请单击**使属性可用于规则和搜索索引编制**。
6. 在**自动检测完成阈值**字段中，设置要检查新属性的连续事件数。

   如果检查连续事件数量时未发现新属性，那么发现过程视为完成，并且禁用**属性自动检测**。您可以随时手动重新启用**属性自动检测**。阈值 0 表示发现过程不断地针对所选日志源类型检查事件。
7. 单击**保存**。

结果

新发现的属性显示在 DSM 编辑器的**属性**选项卡中。

为日志源类型配置日志源自动检测

为日志源类型配置日志源自动检测，这样则不需要为每个实例手动创建一个日志源。日志源自动检测配置还可帮助提高检测共享公共格式的设备的准确性，且避免创建不正确的检测设备，从而提高管道性能。

开始之前

在 QRadar V7.3.2 中，从先前版本升级会启用全局配置设置，这些设置存储在 QRadar 数据库中。此全局设置最初根据 QRadar Console 上 `/opt/qradar/conf/` 目录中 TrafficAnalysisConfig.xml 文件内容进行设置。如果此文件是在升级到 V7.3.2 之前定制的，那么会保留定制。如果部署中每个受管主机上都存在不同的定制，那么这些定制不会转移到全局设置。您仍可以使用配置文件方法来启用按事件处理器的自动检测设置。在**管理 > 系统和许可证管理 > 编辑受管主机 > 组件管理**中，禁用全局自动检测设置。

关于此任务

启用日志源自动检测时，如果创建的定制日志源类型在网络中具有很多实例，则不需要为每个实例手动创建一个日志源。

还可使用 QRadar REST API 或命令行脚本，启用和禁用自动检测哪些日志源类型。如果使用的日志源类型较少，则可配置自动检测哪些日志源，以使检测加速。

如果选择还原为基于文件（非全局）设置，那么仅可使用配置文件来配置自动检测。DSM 编辑器和 REST API 只能使用全局设置。将任何定制自动检测配置移动到全局设置和 DSM 编辑器。

调整自动检测引擎，从而使日志源不会错误地识别为错误类型。在事件不是源自 DSM 相应系统类型的情况下，DSM 仍然错误地将事件识别为其自己的事件时，会出现错误检测。例如，如果事件格式与 DSM 支持的格式相似，或者其包含 DSM 所查找的相同关键字。即使针对将生成事件的系统存在一个 DSM，如果事件很相似，导致不正确的 DSM 如正确的 DSM 一样成功解析事件，也可能会发生错误检测。此 DSM 错误地将事件识别为自己的事件，自动检测引擎创建类型错误的日志源。

例如，如果在 QRadar 部署中同时具有 Linux 和 AIX® 系统，大部分情况下 Linux 会出现此情况。您可以针对 Linux 减小**自动检测的最小成功事件数**或者**自动检测的最小成功事件数**参数值。或者，针对 AIX 增大**自动检测的最小成功事件数**或者**自动检测的最小成功事件数**参数值。

过程

1. 在导航菜单（☰）上，单击**管理**。
2. 在**数据源**部分中单击 **DSM 编辑器**。
3. 从“**选择日志源类型**”窗口选择日志源类型或者创建一个新的日志源类型。
4. 单击**配置**选项卡，然后单击**启用日志源自动检测**。
5. 配置以下参数：

参数	描述
日志源名称模板	输入用于设置自动检测日志源的名称的模板。 可以使用以下两个变量： · **$$DEVICE_TYPE$$** 与日志源类型名称对应。 · **$$SOURCE_ADDRESS$$** 与事件源自的源地址对应。
日志源描述模板	输入用于设置自动检测日志源描述的模板。 可以使用以下两个变量： · **$$DEVICE_TYPE$$** 与日志源类型名称对应。 · **$$SOURCE_ADDRESS$$** 与事件源自的源地址对应。
自动检测的最小成功事件数	针对要发生的自动检测，必须成功解析的来自未知源的最小事件数。
自动检测的最小成功率	针对要发生的自动检测，来自未知源的事件的最低成功解析百分比。
尝试解析限制	放弃自动检测之前尝试的来自未知源的最大事件数。
连续失败的解析限制	来自未知源将放弃自动检测的连续事件数。

6. 单击**保存**。

定制日志源类型

使用 DSM 编辑器来创建和配置定制日志源类型以解析您的事件。 如果为没有受支持的 DSM 的定制应用程序和系统创建日志源类型，那么 QRadar 分析数据的方式与对受支持 DSM 使用的方式相同。

您可以从**日志活动**选项卡选择事件，然后将其直接发送到 DSM 编辑器以进行解析。或者，可以从**管理**选项卡打开 DSM 编辑器以创建并配置新日志源类型。

在 DSM 编辑器的字段中填入正确的结构化数据以解析来自这些事件的相关信息。QRadar 使用**事件类别**和**事件标识**字段将含义映射到事件。“事件标识”是定义事件的必填字段，类别对事件进行进一步划分。您可以将**事件类别**设置为“设备类别”名称，或者可以将其保留为未知。如果您将**事件类别**保留为未知，那么针对为此日志源类型创建的任何事件映射必须将其设置为未知。

使用 DSM 编辑器来映射要从您的事件解析的事件标识/事件类别组合。将事件标识/事件类别组合输入到**事件映射**选项卡中的新条目。您可以选择与您的事件相关的先前创建的 QID 映射条目分类，或单击**选择 QID** 来创建新映射条目。

相关任务

第 71 页的『创建事件映射和分类』

事件映射是用于将事件映射到 QID 的事件标识和类别组合。使用 DSM 编辑器，可创建新的事件映射，以将所有未知事件映射到 QID 映射中的条目。还可以将现有事件重新映射到新创建的事件分类 (QID) 或系统中的现有事件分类。

创建定制日志源类型以解析事件

如果您拥有已导入到 QRadar 中的事件，那么您可以选择希望定制日志源类型所基于的事件并将其直接发送到 DSM 编辑器。

过程

1. 单击**日志活动**选项卡。
2. 暂停传入的结果，然后突出显示一个或多个事件。

   要点: 您只能选择一种登录源类型，且仅会将日志活动中与所选日志源类型匹配的事件自动添加到工作空间。
3. 在导航菜单上，选择**操作 > DSM 编辑器**，然后选择以下某个选项：
   - 如果要解析已知事件，请从列表中选择您的日志源类型。
   - 如果要解析已存储的事件，请单击**新建**。在**日志源类型名称**字段中输入日志源类型的名称并单击**保存**。
4. 在**属性**选项卡中，对要编辑的属性选中**覆盖系统属性**复选框。

下一步做什么

第 59 页的『DSM 编辑器中的属性配置』

相关任务

第 71 页的『创建事件映射和分类』

事件映射是用于将事件映射到 QID 的事件标识和类别组合。使用 DSM 编辑器，可创建新的事件映射，以将所有未知事件映射到 QID 映射中的条目。还可以将现有事件重新映射到新创建的事件分类 (QID) 或系统中的现有事件分类。

第 66 页的『为日志源类型配置属性自动检测』

启用**属性自动检测**时，会自动生成新的属性，以捕获所选日志源类型接收的事件中存在的所有字段。为日志源类型配置新属性的属性自动检测，这样则不需要为每个实例手动创建一个定制属性。

第 66 页的『为日志源类型配置日志源自动检测』

为日志源类型配置日志源自动检测，这样则不需要为每个实例手动创建一个日志源。日志源自动检测配置还可帮助提高检测共享公共格式的设备的准确性，且避免创建不正确的检测设备，从而提高管道性能。

第 69 页的『创建定制属性』

在 DSM 编辑器中，可以为其事件未拟合 IBM QRadar 规范化事件模型的一个或多个日志源类型定义定制属性。例如，一组系统属性可能不会从一些应用程序、操作系统、数据库和其他系统捕获所有相关数据。

DSM 编辑器中的定制属性定义

您可在单独 DSM 中定义定制属性和复用相同属性。在搜索和规则中使用这些属性，并使用这些属性来允许通过用户定义的特定行为将值解析到这些字段中。

在适当情况下，每个定制属性都有一组包含可选择性和数据解析的配置选项。DSM 配置中的每个定制属性定义是一组经过排序的表达式，其中包含表达式类型、表达式、捕获组、可选的可选择性配置以及已启用或已禁用切换按钮。您无法在 DSM 编辑器中的**属性**选项卡上修改定制属性的 **Name**、**Field type**、**Description**、**optimize** 字段或任何高级选项。

在所有 DSM 之间共享定制属性，而从有效内容读取值的特定实施处于 DSM 级别。

要将表达式配置为仅在满足特定条件时才运行，请指定可选择性。

注: 为定制属性的 **Capture Group** 字段分配的值不能大于正则表达式中的捕获组数目。

相关概念

DSM 编辑器中的属性

在 DSM 编辑器中，规范化的属性将与定制属性进行组合并按字母顺序进行排序。

选择性

在 DSM 编辑器中，您可以将运行定制属性限制为特定条件从而获取更好的性能。

以下是限制的类型：

按高级别类别和低级别类别

仅在高级别和低级别类别匹配特定组合时评估属性。例如，仅在事件已知具有高级别类别**认证**和低级别类别**管理注销**时评估属性。

按特定 QID

仅在查看的事件映射到特定 QID 的时评估属性。例如，在事件映射到**登录失败**的 QID 时评估属性。

表达式

您可以在 DSM 编辑器中定义定制属性的表达式。表达式是定义属性行为的一种机制。表达式的主要组件是有效的正则表达式或 JSON。组成表达式的数据取决于属性类型。

对于定制属性，只能从正则表达式中选择一个捕获组。

创建定制属性

在 DSM 编辑器中，可以为其事件未拟合 IBM QRadar 规范化事件模型的一个或多个日志源类型定义定制属性。例如，一组系统属性可能不会从一些应用程序、操作系统、数据库和其他系统捕获所有相关数据。

关于此任务

您可以针对未拟合 QRadar 系统属性的数据创建定制属性。在搜索中使用定制属性，并在规则中对其进行测试。

表 *15.* 定制属性参数

参数	**描述**
名称	创建的定制属性的描述性名称。
字段类型	缺省值为**文本**。 **注:** 从**字段类型**列表选择**数字**或**日期**时，会显示其他字段。
启用此属性以在规则和搜索索引编制中使用	启用时，在事件管道的解析阶段，QRadar 会在事件进入系统时立即尝试从这些事件抽取属性。管道下游的其他组件（如规则、转发概要文件和编制索引）可以使用已抽取的值。属性信息会和其余事件记录一起保留，将其作为搜索或报告一部分检索时，不需要再次抽取。此选项会在检索属性时提高性能，但是在事件解析过程期间会对性能造成负面影响，同时还会影响存储。 未启用时，QRadar 仅在检索或查看事件时才从事件抽取属性。 **注:** 对于要在规则测试或转发概要文件中使用或要用于搜索索引编制的定制属性，必须选中此复选框，因为在事件写入磁盘之前可能会进行规则评估、事件转发和索引编制，所以必须在解析阶段抽取值。

表 *15.* 定制属性参数 *(续)*	
参数	**描述**
使用语言环境的数字格式	从**字段类型**列表选择**数字**时，会显示此字段。如果选中**使用语言环境中的数字格式**复选框，那么必须从列表选择**已抽取数字格式**。
抽取的日期/时间格式	从**字段类型**列表选择**日期**时，会显示此字段。必须提供日期时间模式，此模式与日期时间在原始事件中显示的方式匹配。 例如，对于诸如“Apr 17 2017 11:29:00”的时间戳记，“MMM dd YYYY HH:mm:s”是有效日期时间模式。
语言环境	从**字段类型**列表选择**日期**时，会显示此字段。必须选择事件的语言环境。 例如，如果语言环境为 **英语**，则会将“Apr”识别为月份“April”的简短格式。但是，如果事件显示为法语，且月份标记为“Avr”（表示 Avril），那么将语言环境设置为**法语**，否则代码会将其识别为无效日期。

过程

1. 要添加定制属性，请在 DSM 编辑器中的**属性**选项卡上单击**添加** (**+**)。
2. 要创建新的定制属性定义，请执行下列步骤：
   a) 在“**选择要表示的定制属性定义**”页面上选择**新建**。
   b) 在**创建新的定制属性定义**页面上，输入**名称**、**字段类型**和**描述**字段的值。
   注: 从**字段类型**列表选择**数字**或**日期**时，会显示其他字段。
   c) 如果要在事件进入系统时从其抽取属性，请选中**使此属性用于规则和搜索索引编制**复选框。
   d) 单击**保存**。
3. 要使用现有定制属性，请执行下列步骤：
   a) 在**选择要表示的定制属性定义**页面上，从**过滤器定义**字段搜索现有定制属性。
   b) 单击**选择**以添加定制属性。
4. 要配置定制属性，请执行下列步骤：
   a) 在**属性**选项卡上找到并选择定制属性。定制属性旁会显示词**定制**，以与系统属性区分。
   b) 从**表达式类型**列表选择表达式类型。
   c) 根据在步骤 b 中选择的表达式类型，定义定制属性的有效表达式。
   注:
   - 对于正则表达式，表达式必须是有效的兼容 Java 的正则表达式。仅当在表达式开头使用 (`?i`) 标记时才支持不区分大小写的匹配。(`?i`) 标记保存在日志源扩展 .xml 文件中。要使用其他表达式，例如 (`?s`)，请手动编辑日志源扩展 .xml 文件。
   - 对于 JSON，表达式必须是使用额外带有 /"*<name of sub-field>*" 的 /"*<name of top-level field>*" 格式的路径以捕获存在的子字段。
   - 对于 LEEF 和 CEF，要捕获键/值对的值，将表达式设置为键。要捕获头字段的值，将表达式设置为此头字段的相应保留字。
   d) 如果表达式类型为正则表达式，请选择捕获组。
   e) 可选： 要将表达式限制为针对特定类别运行，请单击**编辑**以选择将其添加到定制属性，并选择**高级类别**和**低级类别**。

f) 可选： 要将表达式限制为针对特定事件或 QID 运行，请单击**选择事件**以搜索特定 QID。

g) 从“**表达式**”窗口中，单击**确定**。

5. 要添加多个表达式并对其重新排序，请执行下列步骤：

a) 单击表达式列表顶部的“添加”(**+**)。

b) 按表达式的运行顺序拖动表达式。

相关信息

有关定义日期时间模式的指导

事件映射

在 DSM 编辑器中，事件映射会显示系统中的所有事件标识和类别组合。

事件映射表示事件标识和类别组合与 QID 记录之间的关联（被称为事件分类）。DSM 从事件抽取事件标识和类别值，然后将其用于查找已映射的事件分类或 QID。事件分类可存储原始事件数据中可能并非逐字存在的事件的额外元数据，例如，人类可以阅读的名称和描述、严重性值或低级类别分配。低级分配和严重性用于搜索和规则定义。

警告: 对于多租户环境，DSM 编辑器中定义的任何用户定义的映射或事件分类信息都会在所有租户之间变为可见。您必须确保在任何事件分类名称或描述中放置任何特定于租户的数据。

创建事件映射和分类

事件映射是用于将事件映射到 QID 的事件标识和类别组合。使用 DSM 编辑器，可创建新的事件映射，以将所有未知事件映射到 QID 映射中的条目。还可以将现有事件重新映射到新创建的事件分类 (QID) 或系统中的现有事件分类。

过程

1. 要添加事件映射，请在 DSM 编辑器的**事件映射**选项卡上单击“添加”(**+**) 图标。
2. 输入**事件标识**和**类别**字段的值。
3. 要创建新的事件分类，请执行以下步骤：

a) 从“**创建新的事件映射**”窗口中，单击**选择事件**。

b) 在“**事件分类**”页面上，单击**创建新的 QID 记录**。

c) 输入**名称**和**描述**字段的值，选择**日志源类型**、**高级类别**、**低级类别**和**严重性**。

d) 单击**保存**以创建新的事件分类。

4. 要使用现有事件分类，请执行以下步骤：

a) 从“**创建新的事件映射**”窗口中，单击**选择事件**。

b) 在“**事件分类**”窗口上，搜索现有事件分类。

c) 选择**高级类别**、**低级类别**、**日志源类型**或 **QID**。结果将显示在**搜索结果**窗格中。

d) 单击**确定**以添加事件类别。

第 7 章 在 QRadar 中使用参考数据

使用参考数据集合以存储和管理想要针对 IBM QRadar 环境中的事件和流关联的业务数据。您可以将业务数据或数据从外部源添加到参考数据集合，然后在 QRadar 搜索、过滤器其、规则测试条件和规则响应中使用数据。

参考数据集合存储在 QRadar 控制台上，但是会定期将集合复制到每个受管主机。要获取最佳数据查找性能，受管主机高速缓存最常引用的数据值。

外部威胁情报数据

您可以使用参考数据集合以将来自第三方供应商的受损指标 (IOC) 数据集成到 QRadar。QRadar 使用 IOC 数据以更快地检测可疑行为，帮助安全分析人员更快地调查威胁和响应事件。

例如，您可以从开放式源代码或基于预订的威胁数据提供商导入 IOC 数据（例如，IP 地址、DNS 名称、URL 和 MD5），并将数据与网络上的事件和事故相关联。

业务数据

参考数据集合可包含特定于组织的业务数据，例如，具有特权系统访问权的用户列表。使用业务数据以创建黑名单和白名单。

例如，使用包含离职员工的用户标识的参考集以阻止他们登录到网络。或者，您可以使用业务数据来构建白名单，仅允许限定的 IP 地址集执行特定功能。

相关概念

IBM QRadar 产品中的功能

参考数据集合的类型

存在不同类型的参考数据集合，每种类型可处理不同级别的数据复杂性。最常用类型是参考集和参考映射。

表 *16.* 参考数据集合的类型

集合的类型	描述	使用量
参考集	唯一值的集合，无特定顺序。 使用 QRadar、命令行或 RESTful API 创建参考集。	使用参考集来将属性值与列表进行比较，例如，IP 地址或用户名。 例如，您可以验证是否将用于登录的 **LoginID** 分配给用户。
参考映射	将唯一键映射到一个值的数据集合。 使用命令行或 RESTful API 创建参考映射。	使用参考映射以验证两个属性值的唯一组合。 例如，要关联网络上的用户活动，您可以创建使用 **LoginID** 参数作为键并使用 **Username** 作为值的参考映射。
集合的参考映射	将一个键映射到多个值的数据集合。每个键唯一并且映射到一个参考集。 使用命令行或 RESTful API 创建集的参考映射。	使用集的参考映射以针对列表验证两个属性值的组合。 例如，要测试专利的授权访问，您可以创建一个集映射，其中将定制事件属性 **Patent ID** 用作键，并将 **Username** 参数用作值。使用集映射来填充授权用户列表。

表 16. 参考数据集合的类型 (续)		
集合的类型	**描述**	**使用量**
映射的参考映射	数据集合，其中将一个键映射到另一个键，然后映射到单个值。每个键唯一并且映射到一个参考映射。 使用命令行或 RESTful API 创建映射的参考映射。	使用映射的参考映射以验证三个属性值的组合。 例如，要测试网络带宽违例，您可以创建一个映射的映射，其中使用 **Source IP** 参数作为第一个键，使用 **Application** 参数作为第二个键，使用 **Total Bytes** 参数作为值。
引用表	与映射的映射类似，但是为第二个键分配一个数据类型。 使用命令行或 RESTful API 创建引用表。	使用引用表以验证三个属性值的组合，其中一个属性是特定数据类型。 例如，您可以创建一个引用表，其将 **Username** 存储为第一个键，将 **SourceIP** 存储为分配了 **cidr** 数据类型的第二个键，并将 **Source Port** 存储为值。

如果想要在 QRadar SIEM 和 QRadar Risk Manager 中使用相同参考数据，那么使用参考集。您无法将其他类型的参考数据集合与 QRadar Risk Manager 一起使用。

参考集概述

在 IBM QRadar 中使用参考集，从而以简单的列表格式存储数据。

您可以使用外部数据（例如，受损指标 (IOC)）填充参考集，或者可以使用其来存储从网络上发生的事件和流收集的业务数据，例如，IP 地址和用户名。

参考集包含可用于搜索、过滤器、规则测试条件和规则响应的唯一值。使用规则来测试参考集是否包含数据元素，或者配置规则响应以向参考集添加数据。例如，您可以创建检测员工访问被禁止的 Web 站点的规则，并配置规则响应以将员工的 IP 地址或用户名添加到参考集。

有关配置规则响应以向参考集添加数据的更多信息，请参阅 *IBM QRadar User Guide*。

相关任务

使用 API 创建参考数据集合

您可以使用应用程序编程接口 (API) 来管理 IBM QRadar 参考数据集合。

添加、编辑和删除参考集

使用参考集可将属性值（例如，IP 地址或用户名）与列表进行比较。您可以将参考集与规则配合使用，以保留监测列表。例如，可以创建规则来检测员工何时访问禁止访问的 Web 站点，然后将该员工的 IP 地址添加到参考集。

关于此任务

将数据添加到参考集之后，**元素数目**和**关联的规则**参数会自动更新。

编辑参考集时，您可更改数据值，但无法更改该参考集所包含的数据类型。

在删除参考集之前，QRadar 会运行依赖关系检查，确定该参考集是否有相关联的规则。

注: 如果您将数据模糊处理技术用于要与参考集数据进行比较的事件属性，请使用字母数字参考集，并添加经模糊处理的数据值。

过程

1. 在导航菜单（☰）上，单击**管理**。

2. 在**系统配置**部分中，单击**参考集管理**。
3. 要添加参考集，请完成下列步骤：
   a) 单击**添加**并配置参数。

   了解有关参考集参数的更多信息：

   下表描述每个用于配置参考集的参数。

表 *17.* 参考集参数

参数	**描述**
名称	参考集名称的最大长度为 255 个字符。
类型	请选择参考元素的数据类型。创建参考集之后，您就无法编辑**类型**元素。 **IP** 类型用于存储 IPv4 地址。**字母数字（忽略大小写）**类型将任何字母数字值自动更改为小写。 要将经模糊处理的事件和流属性与参考数据进行比较，您必须使用字母数字参考集。
元素生存时间	指定参考元素的到期时间。如果选择缺省设置**永远存留**，那么参考元素不会到期。 如果指定时间量，请指出生存时间间隔是基于数据第一次出现的时间，还是基于最后一次出现的时间。 QRadar 定期从参考集中移除已到期的元素（缺省情况下，每 5 分钟移除一次）。
元素到期时间	指定从参考集中移除已到期的参考元素时，如何将这些元素记录在 `qradar.log` 文件中。 **将每个元素记录在单独的日志条目中**选项针对所移除的每个参考元素触发**参考数据元素已到期**日志事件。该事件包含参考集名称和元素值。 **将元素记录在一个日志条目中**选项针对同时移除的所有参考元素触发一个**参考数据元素已到期**日志事件。该事件包含参考集名称和元素值。 **不记录元素**选项不会针对已移除的参考元素触发日志事件。

   b) 单击**创建**。
4. 单击**编辑**或**删除**以处理现有参考集。

   提示： 要删除多个参考集，请使用**快速搜索**文本框来搜索所要删除的参考集，然后单击**删除所列项**。

相关任务

查看参考集的内容

跟踪到期用户帐户

在 IBM QRadar 环境中使用参考数据集合识别过时数据（例如，到期的数据帐户）。

查看参考集的内容

查看参考集中数据元素的相关信息，例如域分配、数据期限及元素最后一次出现在网络中的时间。

过程

1. 在导航菜单（☰）上，单击**管理**。
2. 在**系统配置**部分中，单击**参考集管理**。
3. 选择参考集，然后单击**查看内容**。
4. 单击**内容**选项卡以查看有关每个数据元素的信息。

提示: 您可使用搜索字段来进行过滤，以获取所有与关键字匹配的元素。无法在**生存时间**列中搜索数据。

进一步了解数据元素:

下表描述了针对参考集中的每个数据元素显示的信息。

表 *18.* 参考集数据元素的相关信息

参数	描述
域	有权访问域的租户用户、MSSP 管理员以及未对其分配租户的用户可以查看特定于域的参考数据。所有租户中的用户可以查看共享参考数据。
值	存储在参考集中的数据元素。例如，值可能显示用户名或 IP 地址。
源	如果数据元素是手动添加的，那么显示用户名；如果数据是通过从外部文件中导入添加的，那么显示文件名。如果添加数据元素的目的是对规则做出响应，那么将显示规则名称。
生存时间	从参考集中移除此元素之前的剩余时间。
最后一次进行查看的日期	最后一次在网络上检测到此元素的日期和时间。

5. 单击**引用**选项卡可以查看在规则测试或规则响应中使用参考集的规则。

表 *19.* “内容”选项卡参数

参数	描述
规则名称	配置为使用参考集的规则的名称。
组	规则所属的组。
类别	显示规则是定制规则还是异常检测规则。
类型	显示**事件**、**流**、**一般**或**攻击**，以指示测试该规则所依据的数据类型。
已启用	必须对定制规则引擎启用规则，才能对其进行评估。
响应	针对此规则配置的响应。
源	**系统**指示缺省规则。 **已修改**指示已定制缺省规则。 **用户**指示用户创建的规则。

6. 要查看或编辑关联的规则，请在**引用**列表中双击该规则，并完成规则向导。

将元素添加到参考集

当您希望 IBM QRadar 将属性与元素值进行比较时，请将元素添加到参考集。使用 QRadar 可以将元素手动添加到参考集，或者从 `.csv` 文件导入元素。

开始之前

要导入元素，请确保 `.csv` 文件存储在本地。

关于此任务

您可以将参考数据分配给特定的域。特定于域的参考数据可以由有权访问域的租户用户、MSSP 管理员以及未获分配租户的用户查看。所有租户中的用户都可以查看共享的参考数据。例如，非管理员 MSSP 用户可以查看分配给某个域的参考数据。

过程

1. 在导航菜单（☰）上，单击**管理**。
2. 在**系统配置**部分中，单击**参考集管理**。
3. 选择要将元素添加到的参考集，然后单击**查看内容**。
4. 单击**内容**选项卡。
5. 要手动添加数据元素，请完成下列步骤：
   a) 单击**添加**并配置参数。

      有效端口值介于 0 与 65535 之间。有效 IP 地址介于 0 与 255.255.255.255 之间。

      注： 如果您将数据模糊处理技术用于要与参考集数据进行比较的事件属性，那么必须使用包含已进行模糊处理的数据值的字母数字参考集。

   b) 单击**添加**。
6. 要从 .csv 文件添加元素，请完成下列步骤：
   a) 单击**导入**。
   b) 单击**选择文件**并进行浏览，以选择要导入的 .csv 文件。

      .csv 文件格式必须是：所有的项位于一行并以逗号分隔，或者每个项各占一行。当每个项各占一行时，不需要定界符。

   c) 选择要将参考集数据添加到的**域**。
   d) 单击**导入**。
      导入操作会将该文本文件的内容添加到参考集。

从参考集中导出元素

希望在报告中包含信息或者与未使用 IBM QRadar 的人共享信息时，将参考集元素导出到 .csv 文件。

过程

1. 在导航菜单（☰）上，单击**管理**。
2. 在**系统配置**部分中，单击**参考集管理**。
3. 选择您要导出的参考集，然后单击**查看内容**。
4. 单击**内容**选项卡，然后单击**导出**。
5. 选择是立即打开文件，还是保存文件，然后单击**确定**。

从参考集中删除元素

将元素添加到错误的参考集时，或者不再需要将元素与其他 IBM QRadar 属性比较时，可能需要从参考集删除元素。例如，您可能需要移除错误地添加到资产排除黑名单的资产。

过程

1. 在导航菜单（☰）上，单击**管理**。
2. 在**系统配置**部分中，单击**参考集管理**。
3. 选择包含您要删除的元素的参考集，然后单击**查看内容**。
4. 单击**内容**选项卡并选择下列其中一个选项：
   - 要删除单个元素，请从列表中选择该元素，然后单击**删除**。
   - 要删除多个元素，请使用搜索框过滤列表以仅显示要删除的元素，然后单击**删除所列项**。

使用 API 创建参考数据集合

您可以使用应用程序编程接口 (API) 来管理 IBM QRadar 参考数据集合。

过程

1. 使用 Web 浏览器访问 `https://<Console IP>/api_doc`，并作为管理员登录。
2. 选择 IBM QRadar API 的最新迭代。
3. 选择 `/reference_data` 目录。
4. 要创建新的参考集，请执行下列步骤：
   a) 选择 `/sets`。
   b) 单击 **POST** 并在**值**字段中输入相关信息。

   了解有关创建参考集的参数的更多信息：

   下表提供有关创建参考集所需的参数的信息：

表 *20.* 参数 - 参考集					
参数	**Type**	**值**	**数据类型**	**MIME 类型**	**样本**
element_type	查询	（必需）	字符串	文本/纯文本	String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>
name	查询	（必需）	字符串	文本/纯文本	字符串
fields	查询	（可选）	字符串	文本/纯文本	field_one (field_two, field_three), field_four
time_to_live	查询	（可选）	字符串	文本/纯文本	字符串
timeout_type	查询	（可选）	字符串	文本/纯文本	String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>

   c) 单击**开始试用！**以完成创建参考数据集合和查看结果。
5. 要创建新的参考映射，请执行下列步骤：
   a) 单击 `/maps`。
   b) 单击 **POST** 并在**值**字段中输入相关信息。

   了解有关创建参考映射的参数的更多信息：

   下表提供有关创建参考映射所需的参数的信息：

表 *21.* 参数 - 参考映射					
参数	**Type**	**值**	**数据类型**	**MIME 类型**	**样本**
element_type	查询	（必需）	字符串	文本/纯文本	String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>
name	查询	（必需）	字符串	文本/纯文本	字符串

表 21. 参数 - 参考映射 (续)					
参数	**Type**	**值**	**数据类型**	**MIME 类型**	**样本**
fields	查询	（可选）	字符串	文本/纯文本	field_one (field_two, field_three), field_four
key_label	查询	（可选）	字符串	文本/纯文本	字符串
time_to_live	查询	（可选）	字符串	文本/纯文本	字符串
timeout_type	查询	（可选）	字符串	文本/纯文本	String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>
value_label	查询	（可选）	字符串	文本/纯文本	字符串

c) 单击**开始试用！**以完成创建参考数据集合和查看结果。

6. 要创建新的集参考映射，请执行下列步骤：

a) 选择 `/map_of_sets`。

b) 单击 **POST** 并在**值**字段中输入相关信息。

了解有关创建集的参考映射的参数的更多信息：

下表提供有关创建集的参考映射所需的参数的信息：

表 22. 参数 - 集的参考映射					
参数	**Type**	**值**	**数据类型**	**MIME 类型**	**样本**
element_type	查询	（必需）	字符串	文本/纯文本	String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>
name	查询	（必需）	字符串	文本/纯文本	字符串
fields	查询	（可选）	字符串	文本/纯文本	field_one (field_two, field_three), field_four
key_label	查询	（可选）	字符串	文本/纯文本	字符串
time_to_live	查询	（可选）	字符串	文本/纯文本	字符串
timeout_type	查询	（可选）	字符串	文本/纯文本	String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>
value_label	查询	（可选）	字符串	文本/纯文本	字符串

c) 单击**开始试用！**以完成创建参考数据集合和查看结果。

7. 要创建新的参考表或映射的映射，请执行下列步骤：

a) 单击 `/tables`。

b) 单击 **POST** 并在**值**字段中输入相关信息。

了解有关创建参考表或映射的映射所需的参数的更多信息：

下表提供有关创建参考表或映射的映射所需的参数的信息：

表 23. 参数 - 参考表

参数	Type	值	数据类型	MIME 类型	样本
element_type	查询	（必需）	字符串	文本/纯文本	String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>
name	查询	（必需）	字符串	文本/纯文本	字符串
fields	查询	（可选）	字符串	文本/纯文本	field_one (field_two, field_three), field_four
key_name_types	查询	（可选）	数组	application/ json	[{ "element_type": "String <one of: ALN, NUM, IP, PORT, ALNIC, DATE>", "key_name": "String" }]
outer_key_label	查询	（可选）	字符串	文本/纯文本	字符串
time_to_live	查询	（可选）	字符串	文本/纯文本	字符串
timeout_type	查询	（可选）	字符串	文本/纯文本	String <one of: UNKNOWN, FIRST_SEEN, LAST_SEEN>

c) 单击**开始试用！**以完成创建参考数据集合和查看结果。

相关概念

参考集概述

使用参考数据收集的示例

这些示例显示如何使用参考数据收集，来追踪并存储您想要在 QRadar 搜索、过滤器、规则测试条件和规则响应中使用的数据。

跟踪到期用户帐户

在 IBM QRadar 环境中使用参考数据集合识别过时数据（例如，到期的数据帐户）。

关于此任务

缺省情况下，参考数据保留在 QRadar 中，直到将其移除。但是，创建参考数据集合时，可配置 QRadar 以在指定时间段后移除数据。

数据元素到期时，QRadar 会自动删除参考数据集合中的值，并触发事件以跟踪到期情况。

过程

1. 创建参考集以跟踪用户自上次登录以来的时间。
   a) 设置**元素的生存时间**以表示未使用帐户被视为到期之前的时间段。
   b) 选择**自上次显示**按钮。
2. 创建定制事件规则以将登录数据（例如，**username**）添加到参考集中。

注: QRadar 跟踪每个数据元素的**上次显示的日期**。如果未在生存时间内为特定用户添加任何数据，参考集数据元素到期，会触发**参考数据到期**事件。事件包含到期的参考集名称和用户名。

3. 使用**日志活动**选项卡以跟踪**参考数据到期**事件。

下一步做什么

在搜索、过滤器、规则测试条件和规则响应中使用参考集数据。

相关任务

添加、编辑和删除参考集

从外部源集成动态数据

大型企业组织可以使用参考数据集合来与管理 IBM QRadar 部署的安全团队共享有关其 IT 资产的信息。

例如，信息技术 (IT) 团队维护资产管理数据库，其中包含有关所有网络资产的信息。某些信息（例如，Web 服务器的 IP 地址）频繁更改。

每周，IT 团队导出在网络中部署的所有 Web 服务器的 IP 地址列表一次，并向安全团队提供此列表。安全团队将列表导入到参考集，然后可用于规则、搜索和报告从而向 QRadar 处理的事件和流提供更多上下文。

第 8 章 用户信息源配置

将 IBM QRadar 系统配置为从 Identity and Access Management 端点收集用户和组信息。

QRadar 使用从端点收集的信息来丰富与网络上发生的流量和事件关联的用户信息。

相关概念

IBM QRadar 产品中的功能

用户信息源概述

您可以配置用户信息源来启用从 Identity and Access Management 端点进行用户信息收集。

Identity and Access Management 端点是用于收集和管理电子用户身份、组成员资格和访问许可权的产品。这些端点称为用户信息源。

使用以下实用程序来配置和管理用户信息源：

- **Tivoli Directory Integrator** - 必须在非 IBM QRadar 主机上安装并配置 Tivoli® Directory Integrator。
- **UISConfigUtil.sh** - 此实用程序用于创建、检索、更新或删除用户信息源。可以通过 Tivoli Directory Integrator 服务器来使用用户信息源集成 IBM QRadar SIEM。
- **GetUserInfo.sh** - 此实用程序用于从用户信息源收集用户信息并将信息存储在参考数据集合中。可以使用此实用程序按需或按计划收集用户信息。

用户信息源

用户信息源是可配置组件，用于启用与端点的通信以检索用户和组信息。

IBM QRadar 系统支持以下用户信息源：

表 *24.* 支持的信息源

信息源	收集的信息
Microsoft Windows Active Directory (AD) V2008 - Microsoft Windows AD 是对使用 Windows 网络的所有用户和计算机进行认证和授权的目录服务。	· full_name · user_name · user_principal_name · family_name · given_name · account_is_disabled · account_is_locked · password_is_expired · password_can_not_be_changed · no_password_expired · password_does_not_expire
IBM Security Access Manager (ISAM) V7.0 - ISAM 是企业 Web、客户机/服务器和现有应用程序的认证和授权解决方案。有关更多信息，请参阅 IBM Security Access Manager (ISAM) 文档。	· name_in_rgy · first-name · last-name · account_valid · password_valid

表 *24.* 支持的信息源 *(续)*	
信息源	**收集的信息**
IBM Security Identity Manager (ISIM) V6.0 - ISIM 提供软件和服务以部署基于策略的供应解决方案。本产品将为员工、承包商和 IBM 业务合作伙伴供应其所需的应用程序访问权的过程自动化，无论是在封闭式企业环境中还是整个虚拟或扩展企业内都如此。有关更多信息，请参阅 IBM Security Integration Manager (ISIM) 文档。	· 全名 · DN

用户信息的引用数据集合

本主题提供有关引用数据集合如何存储从用户信息源收集的数据的信息。

在 IBM QRadar SIEM 从用户信息源收集信息时，其自动创建一个引用数据集合来存储信息。引用数据集合的名称派生自用户信息源组名。例如，从 Microsoft Windows AD 收集的引用数据集合可命名为 Domain Admins。

引用数据集合类型为“映射的映射”。在“映射的引用映射”中，数据存储在记录中，此记录将一个键映射到另一个键，然后映射到单个值。

例如：

```
·#
·# Domain Admins
·# key1,key2,data
·smith_j,Full Name,John Smith
·smith_j,account_is_disabled,0
·smith_j,account_is_locked,0
·smith_j,account_is_locked,1
·smith_j,password_does_not_expire,1
```

有关引用数据集合的更多信息，请参阅“引用数据集合技术说明”。

集成工作流程示例

在参考数据集合中收集和存储用户和组信息后，可通过多种方式在 IBM QRadar SIEM 中使用数据。

您可以创建有意义的报告和警报，遵循公司的安全策略描述用户。

请考虑以下示例：

为确保特权 ISIM 用户所执行的活动符合安全策略，您可以完成以下任务：

创建日志源以针对从中收集日志的每个 ISIM 服务器收集和解析审计数据：有关如何创建日志源的更多信息，请参阅 *Managing Log Sources Guide*。

1. 针对 ISIM 服务器创建用户信息源并收集 ISIM 管理员用户组信息。此步骤会创建一个名为 ISIM 管理员的参考数据集合。
2. 配置构建块以测试源 IP 地址是 ISIM 服务器并且用户名在 ISIM 管理员参考数据集合中列出的事件。有关构建块的更多信息，请参阅产品的《用户指南》。
3. 创建使用定制构建块作为过滤器的事件搜索。有关事件搜索的更多信息，请参阅产品的 *IBM QRadar User Guide*。
4. 创建使用定制事件搜索的定制报告，从而生成有关特权 ISIM 用户的审计活动的每日报告。这些生成的报告指示是否有任何 ISIM 管理员活动违反安全策略。有关报告的更多信息，请参阅产品的 *IBM QRadar User Guide*。

注: 如果想要收集应用程序安全日志，必须创建“设备支持模块”(DSM)。有关更多信息，请参阅《*IBM QRadar DSM* 配置指南》。

第 9 章 IBM X-Force 集成

IBMX-Force 安全专家使用一系列国际数据中心收集成千上万的恶意软件样本，分析 Web 页面和 URL，并运行分析来对可能恶意的 IP 地址和 URL 进行分类。IBM X-Force Exchange 是可在 IBM QRadar 中使用的用于共享此数据的平台。

相关概念

IBM QRadar 产品中的功能

X-Force Threat Intelligence 订阅源

您可以将 IBM X-Force Exchange 数据集成到 IBM QRadar 中，从而在环境中的不当活动威胁网络的稳定性之前，通过识别该活动并进行补救来帮助组织提早防范兴起的威胁。

例如，您可以识别以下类型的事故并排列其优先顺序：

- 对动态 IP 地址范围的一系列登录尝试
- 与业务合作伙伴门户网站的匿名代理连接
- 内部端点与已知僵尸网络命令和控制之间的连接
- 端点与已知恶意软件分发站点之间的通信

注： IBM X-Force 集成允许在 QRadar 关联规则和 AQL 查询中使用 X-Force Threat Intelligence 数据。不包括对 IBM X-Force Exchange REST API 的访问。

仪表板上的 X-Force 数据

“威胁和安全性监视”仪表板上的**“因特网威胁信息中心”**窗口小部件使用 X-Force 数据来提供关于安全问题、每日威胁评估、安全新闻和威胁存储库的最新意见。

该仪表板窗口小部件使用嵌入的 RSS 订阅源在仪表板窗口小部件中显示 X-Force 数据。QRadar Console 必须有权访问因特网以接收来自 X-Force 更新服务器 (www.iss.net) 的数据。

该仪表板提供四个 AlertCon 威胁级别图像，以提供当前威胁级别的可视指示器。

表 *25. AlertCon* 威胁级别

级别	类型	描述
1	正常威胁	组成不受保护的网络的正常活动，在 QRadar 连接到因特网后持续数分钟到数小时。
2	加强警戒	漏洞或对计算机网络存在的联机威胁，需要进行漏洞评估或执行纠正行动。
3	集中攻击	属于因特网攻击目标的特定弱点和漏洞，需要立即采取防御行动。
4	灾难性威胁	网络中的紧急安全情况，需要立即采取集中防御行动。此状况可能即将发生或持续发生。

有关当前威胁级别的更多信息，请单击**了解更多信息**链接以打开 IBM X-Force Exchange Web 站点上的**“当前威胁活动”**页面。

要查看当前意见摘要，请单击意见旁边的箭头图标。要查看完整的意见，请单击意见链接。

IBM Security Threat Content 应用程序

IBM Security App Exchange (https://exchange.xforce.ibmcloud.com/hub) 上的 **IBM Security Threat Content** 应用程序包含旨在与 X-Force 订阅源数据配合使用的规则、构建块和定制属性。

X-Force 数据包含潜在恶意的 IP 地址和 URL 列表，其中具有对应的威胁评分。您可以使用 X-Force 规则来自动标记包含地址的任何安全事件或网络活动数据，并排列事件优先顺序，然后再开始调查这些事件或数据。

以下列表显示了可以使用 X-Force 规则识别的事件类型：

- **当 *[source IP|destinationIP|anyIP]* 属于以下任一 *[remote network locations]* 时**
- **当 X-Force 将 *[this host property]* 分类为 *[Anonymization Servers|Botnet C&C|DynamicIPs|Malware|ScanningIPs|Spam]*（置信度值 *[equal to] [this amount]*）时**
- **当 X-Force 将 *[this URL property]* 分类为 *[Gambling|Auctions|Job Search|Alcohol|Social Networking|Dating]* 时**

当启用 X-Force Threat Intelligence 订阅源来与 **IBM Security Threat Content** 应用程序配合使用时，QRadar 每天下载大约 30 MB 的 IP 声誉数据。

安装 IBM Security Threat Content 应用程序

IBM Security Threat Content 应用程序包含专门为了与 X-Force 数据配合使用而设计的 IBM QRadar 内容，例如规则、构建块和定制属性。增强内容可帮助您识别环境中的不良活动，进行补救，避免其威胁到网络稳定性。

开始之前

从 IBM Security App Exchange (https://exchange.xforce.ibmcloud.com/hub) 下载 IBM Security Threat Content 应用程序。

关于此任务

要在 QRadar 规则、攻击或事件中使用 X-Force 数据，必须配置 IBM QRadar，使其自动将数据从 X-Force 服务器装入到 QRadar 设备中。

要在本地装入 X-Force 数据，请在系统设置中启用“X-Force 威胁情报”订阅源。当 X-Force 启动时，如果有新的信息可供使用，那么 IP 地址声誉或 URL 数据库就会更新。这些更新会合并到它们自己的数据库中，内容会从 QRadar Console 复制到部署中的所有本地受管主机。

X-Force 规则在产品中保持可见，即使稍后将 **IBM Security Threat Content** 应用程序卸载也是如此。

过程

1. 在导航菜单（☰）上，单击**管理**。
2. 在**系统配置**部分中，单击**扩展管理**。
3. 完成下列步骤，将 **IBM Security Threat Content** 应用程序上载至 QRadar 控制台：
   a) 单击**添加**。
   b) 单击**浏览**以查找该扩展。
   c) 单击**立即安装**以安装该扩展，不查看内容。
   d) 单击**添加**。
4. 要查看该扩展的内容，请从扩展清单中选中该扩展，然后单击**更多详细信息**。
5. 要安装该扩展，请完成下列步骤：
   a) 从列表选择该扩展，然后单击**安装**。
   b) 如果该扩展没有数字签名，或者它已签署，但是该签名与 IBM Security 认证中心 (CA) 没有关联，那么您必须确认仍要安装。请单击**安装**以继续安装。
   c) 复查安装操作对系统所作的更改。

d) 选择**覆盖**或**保留现有数据**，以指定如何处理现有的内容项。

e) 单击**安装**。

f) 复查安装摘要，然后单击**确定**。

规则随即出现在“**规则列表**”窗口中的**威胁**组下。它们必须先启用才能使用。

适用于 QRadar 的 IBM X-Force Exchange 插件

IBM X-Force Exchange 是安全分析人员、网络安全性专家和安全性运营中心团队所使用的威胁情报的共享平台。

IBM X-Force Exchange (XFE) 查看可提供在 IBM X-Force Exchange Web 站点上搜索 QRadar 中找到的 IP 地址、URL、CVE 和 Web 应用程序信息的选项。
例如，您可右键单击来自 QRadar 事件的 URL，以查看 X-Force Exchange 包含哪些有关此 URL 的数据。

您还可使用右键单击查找选项将来自 QRadar 搜索、攻击和规则的 IP 地址或 URL 数据提交至公共集合或专用集合。此集合可将这些信息存储在一处，以便您将这些数据用于进一步研究。

这些集合还包含充当百科样式的记事本的部分，您可在其中添加相关注释或任何自由文本。您可使用此集合来保存 X-Force 报告、文本注释或任何其他内容。X-Force 报告包含报告保存时的版本和指向最新版本报告的链接。

第 10 章 流源

对于 IBM QRadar 设备，QRadar 自动针对设备上的物理端口添加缺省流源，并且包含缺省 NetFlow 流源。

如果在自己的硬件上安装 QRadar，那么 QRadar 尝试自动检测并添加任何物理设备的缺省流源，例如，网络接口卡 (NIC)。在分配 IBM QRadar QFlow Collector 时，QRadar 包含缺省 NetFlow 流源。

流源分类为内部或外部：

内部流源
包含在受管主机上安装的任何其他硬件，例如，网络接口卡 (NIC)。根据受管主机的硬件配置，内部流源可能包含以下源：

- 网络接口卡
- Napatech 接口

外部流源
包含将流发送到 QRadar QFlow Collector 的任何外部流源。如果 QRadar QFlow Collector 收到多个流源，那么可为每个流源分配一个不同的名称。在同一 QRadar QFlow Collector 收到外部流数据时，不同名称可帮助相互区分外部流源数据。

外部流源可能包含以下源：

- NetFlow
- IPFIX
- sFlow
- J-Flow
- Packeteer
- 流日志 文件

QRadar SIEM 可使用电子欺骗或非非电子欺骗方法转发外部流源数据：

电子欺骗
将从流源收到的入站数据重新发送到次要目标。为确保将流源数据发送到次要目标，请将流源配置中的**监视接口**参数配置为接收数据的端口（管理端口）。在使用特定接口时，QRadar QFlow Collector 使用混合方式捕获来获取流源数据，而不是端口 2055 上的缺省 UDP 侦听端口。因此，QRadar QFlow Collector 可捕获流源包并转发数据。

非电子欺骗
对于非电子欺骗方法，将流源配置中的**监视接口**参数配置为任何。QRadar QFlow Collector 打开侦听端口，这是配置为**监视端口**以接受流源数据的端口。将处理数据并转发到另一个流源目标。源流数据的源 IP 地址将成为 QRadar SIEM 系统的 IP 地址，而不是发送数据的源路由器。

流源的类型

IBM QRadar QFlow Collector 可处理来自多个源的流，这些源分类为内部或外部源。

内部流源

通过连接到 SPAN 端口或网络 TAP 包含包数据的源被称为内部源。这些源向 Flow Collector 上的监视端口提供原始包数据，其中包详细信息将转换为流所记录。

QRadar 不会保存整个包有效内容。而是捕获流的快照（被称为有效内容或内容捕获），其中包含从通信开始的包。

来自内部源的流集合通常需要专用 Flow Collector。

外部流源

QRadar 还支持外部流源，例如，发送 NetFlow、sFlow、J-Flow 和 Packeteer 数据的路由器。

外部源不需要尽可能高的 CPU 利用率以进行处理，因此您可以直接将它们发送到 流处理器。在此配置中，您可能有一个专用流收集器和流处理器，它们两个都接收和创建流数据。

NetFlow

NetFlow 是 Cisco Systems 开发的专有统计技术。NetFlow 监视流经交换机或路由器的流量，解释使用的客户机、服务器、协议和端口，统计字节和包数量，并将此数据发送给 NetFlow 收集器。

从 NetFlow 发送数据的过程通常被称为 NetFlow 数据导出 (NDE)。您可以配置 IBM QRadar 以接受 NDE 并因此成为 NetFlow 收集器。QRadar 支持 NetFlow V1、V5、V7 和 V9。有关 NetFlow 的更多信息，请参阅 Cisco Web 站点 (http://www.cisco.com)。

在 NetFlow 扩展监视的网络量时，NetFlow 使用无连接协议 (UDP) 来交付 NDE。从交换机或路由器发送 NDE 后，将清除 NetFlow 记录。因为使用 UDP 来发送此信息并且不保证数据交付，NetFlow 记录不准确记录并降低了警报能力。这可能导致流量和双向流的表示不准确。

在针对 NetFlow 配置外部流源时，必须执行以下任务：

- 确保配置相应的防火墙规则。如果更改 IBM QRadar QFlow Collector 配置中的**外部流源监视端口**参数，那么还必须更新防火墙访问配置。
- 确保针对 QRadar QFlow Collector 配置相应的端口。

如果使用 NetFlow V9，确保来自 NetFlow 源的 NetFlow 模板包含以下字段：

- FIRST_SWITCHED
- LAST_SWITCHED
- PROTOCOL
- IPV4_SRC_ADDR
- IPV4_DST_ADDR
- L4_SRC_PORT
- L4_DST_PORT
- IN_BYTES 或 OUT_BYTES
- IN_PKTS 或 OUT_PKTS
- TCP_FLAGS（仅限 TCP 流）

针对 NetFlow V9 支持以下 VLAN 字段。

- vlanId
- postVlanId
- dot1qVlanId
- dot1qPriority
- dot1qCustomerVlanId
- dot1qCustomerPriority
- postDot1qVlanId
- postDotqCustomerVlanId
- dot1qDEI
- dot1qCustomerDEI

IPFIX

Internet Protocol Flow Information Export (IPFIX) 是一种记帐技术。IPFIX 监视流经交换机或路由器的流量，解释使用的客户机、服务器、协议和端口，统计字节和包数量，并将此数据发送给 IPFIX 收集器。

IBM Security Network Protection XGS 5000（下一代入侵防御系统 (IPS)）是以 IPFIX 流格式发送流量的设备示例。

发送 IPFIX 数据的过程通常被称为 NetFlow 数据导出 (NDE)。IPFIX 提供比 NetFlow V9 更多的流信息和更深入的洞察。您可以配置 IBM QRadar 以接受 NDE 并因此成为 IPFIX 收集器。IPFIX 使用“用户数据报协议”(UDP) 来交付 NDE。在从 IPFIX 转发设备发送 NDE 后，可能会清除 IPFIX 记录。

要配置 QRadar 以接受 IPFIX 流量，必须添加 NetFlow 流源。NetFlow 流源使用相同过程来处理 IPFIX 流。

QRadar 系统可能包含缺省 NetFlow 流源；因此，您无需配置 NetFlow 流源。要确认系统包含缺省 NetFlow 流源，请在**管理**选项卡上，选择**流源**。如果在流源列表中列出 **default_Netflow**，那么已配置 IPFIX。

在针对 IPFIX 配置外部流源时，必须执行以下任务：

- 确保配置相应的防火墙规则。如果更改 IBM QRadar QFlow Collector 配置中的**外部流源监视端口**参数，那么还必须更新防火墙访问配置。
- 确保针对 QRadar QFlow Collector 配置相应的端口。
- 确保来自 IPFIX 源的 IPFIX 模板包含以下列出 IANA 的信息元素：
  - protocolIdentifier (4)
  - sourceIPv4Address (8)
  - destinationIPv4Address (12)
  - sourceTransportPort (7)
  - destinationTransportPort (11)
  - octetDeltaCount (1) 或 postOctetDeltaCount (23)
  - packetDeltaCount (2) 或 postPacketDeltaCount (24)
  - tcpControlBits (6)（仅限 TCP 流）
  - flowStartSeconds (150)、flowStartMilliseconds (152) 或 flowStartDeltaMicroseconds (158)
  - flowEndSeconds (151)、flowEndMilliseconds (153) 或 flowEndDeltaMicroseconds (159)

针对 IPFIX 支持以下 VLAN 字段。

- vlanId
- postVlanId
- dot1qVlanId
- dot1qPriority
- dot1qCustomerVlanId
- dot1qCustomerPriority
- postDot1qVlanId
- postDotqCustomerVlanId
- dot1qDEI
- dot1qCustomerDEI

针对 IPFIX 支持以下 MPLS 字段。

- mplsTopLabelType
- mplsTopLabelIPv4Address
- mplsTopLabelStackSection
- mplsLabelStackSection2
- mplsLabelStackSection3

- mplsLabelStackSection4
- mplsLabelStackSection5
- mplsLabelStackSection6
- mplsLabelStackSection7
- mplsLabelStackSection8
- mplsLabelStackSection9
- mplsLabelStackSection10
- mplsVpnRouteDistinguisher
- mplsTopLabelPrefixLength
- mplsTopLabelIPv6Address
- mplsPayloadLength
- mplsTopLabelTTL
- mplsLabelStackLength
- mplsLabelStackDepth
- mplstopLabelExp
- postMplsTopLabelExp
- pseudoWireType
- pseudoWireControlWord
- mplsLabelStackSection
- mplsPayloadPacketSection
- sectionOffset
- sectionExportedOctets

有关这些 MPLS 字段的更多信息，请参阅 IP Flow Information Export (IPFIX) Entities (https://www.iana.org/assignments/ipfix/ipfix.xhtml)。

sFlow

sFlow 是多供应商和用户的采样技术标准，可同时提供所有接口上应用程序级别流量流的持续监视。

sFlow 将接口计数器和流样本组合到 sFlow 数据报，此数据包将通过网络发送到 sFlow 收集器。IBM QRadar 支持 sFlow V2、4 和 5。sFlow 流量基于采样数据，因此可能不表示所有网络流量。有关更多信息，请访问 sFlowWeb 站点 (www.sflow.org)。

sFlow 使用无连接协议 (UDP)。在从交换机或路由器发送数据时，将清除 sFlow 记录。因为使用 UDP 来发送此信息并且不保证数据交付，sFlow 记录不准确记录并降低了警报能力。这可能导致流量和双向流的表示不准确。

在针对 sFlow 配置外部流源时，必须执行以下任务：

- 确保配置相应的防火墙规则。
- 确保针对 QRadar VFlow Collector 配置相应的端口。

J-Flow

Juniper Networks 使用的专有统计技术，允许您收集 IP 流统计信息。J-Flow 支持您将数据导出到 J-Flow 收集器上的 UDP 端口。使用 J-Flow，您还可以在路由器或接口上启用 J-Flow 以收集网络上特定位置的网络统计信息。

请注意，J-Flow 流量基于采样的数据，因此可能不代表所有网络流量。有关 J-Flow 的更多信息，请访问 Juniper Networks Web 站点 (www.juniper.net)。

J-Flow 使用无连接协议 (UDP)。在从交换机或路由器发送数据时，将清除 J-Flow 记录。因为使用 UDP 来发送此信息并且不保证数据交付，J-Flow 记录不准确记录并降低了警报能力。这可能导致流量和双向流的表示不准确。

在针对 J-Flow 配置外部流源时，您必须：

- 确保配置相应的防火墙规则。
- 确保针对 IBM QRadar QFlow Collector 配置相应的端口。

针对 J-Flow 支持以下 VLAN 字段。

- vlanId
- postVlanId
- dot1qVlanId
- dot1qPriority
- dot1qCustomerVlanId
- dot1qCustomerPriority
- postDot1qVlanId
- postDotqCustomerVlanId
- dot1qDEI
- dot1qCustomerDEI

Packeteer

Packeteer 设备收集、聚集和存储网络性能数据。在针对 Packeteer 配置外部流源后，您可以将流信息从 Packeteer 设备发送到 IBM QRadar。

Packeteer 使用无连接协议 (UDP)。在从交换机或路由器发送数据时，将清除 Packeteer 记录。因为使用 UDP 来发送此信息并且不保证数据交付，Packeteer 记录不准确记录并降低了警报能力。可能发生流量和双向流的表示不准确。

要将 Packeteer 配置为外部流源，必须执行以下任务：

- 确保配置相应的防火墙规则。
- 确保配置 Packeteer 设备以导出流详细信息记录并将 IBM QRadar QFlow Collector 配置为数据导出的目标。
- 确保针对 QRadar QFlow Collector 配置相应的端口。
- 确保 QRadar QFlow Collector 可自动检测 Packeteer 设备的类标识。
- 有关更多信息，请参阅“将 Packeteer 设备映射到 QRadar 技术说明”。

Flowlog 文件

从 IBM QRadar 流日志生成 Flowlog 文件。

Napatech 接口

如果在 IBM QRadar 系统上安装了 Napatech 网络适配器，那么将在 QRadar 用户界面上显示 **Napatech 接口**以作为可配置的基于包的流源。Napatech 网络适配器为您的网络提供下一代可编程、智能网络适配器。有关更多信息，请参阅 Napatech 文档。

添加或编辑流源

使用“**流源**”窗口可添加流源。

过程

1. 在导航菜单（☰）上，单击**管理**。
2. 在**数据源**部分中的**流**下，单击**流源**。
3. 执行下列其中一项操作：

- 要添加流源，请单击**添加**。
- 要编辑流源，请选择流源，然后单击**编辑**。

4. 要从现有流源创建此流源，请选中**从现有流源构建**复选框，然后从**用作模板**列表选择流源。
5. 对于**流源名称**，输入名称。

   提示: 如果外部流源同时也是物理设备，请使用设备名称作为流源名称。如果该流源不是物理设备，请使用可识别的名称。

   例如，如果要使用 IPFIX 流量，请输入 **ipf1**。如果要使用 NetFlow 流量，请输入 **nf1**。
6. 从**流源类型**列表选择流源，并配置属性。
   - 如果选择**流日志文件**选项，请确保为**源文件路径**参数配置流日志文件位置。
   - 如果在**流源类型**参数中选择 **JFlow**、**Netflow**、**Packeteer**、**FDR** 或 **sFlow** 选项，请确保为**监视端口**参数配置可用的端口。

     网络中配置的第一个 NetFlow 流源的缺省端口为 2055。对于其他每个 NetFlow 流源，缺省端口号按 1 递增。例如，第二个 NetFlow 流源的缺省 NetFlow 流源端口为 2056。
   - 如果选择 **Napatech 接口**选项，请输入要分配给流源的**流接口**。

     限制: 只有在系统上已安装 Napatech 网络适配器的情况下，才会显示 **Napatech 接口**选项。
   - 如果选择**网络接口**选项，那么对于**流接口**，请为每个以太网接口仅配置一个日志源。

     限制: 不能将不同流类型发送到同一个端口。
7. 如果网络上的流量配置为入站流量与出站流量使用不同的路径，请选中**启用非对称流**复选框。
8. 单击**保存**。
9. 在**管理**选项卡上，单击**部署更改**。

启用和禁用流源

使用“**流源**”窗口，可启用或禁用流源。

过程

1. 在导航菜单（☰）上，单击**管理**。
2. 在**数据源**部分中的**流**下，单击**流源**。
3. 选择要启用或禁用的流源，然后单击**启用/禁用**。
4. 在**管理**选项卡上，单击**部署更改**。

删除流源

使用“**流源**”窗口删除流源。

过程

1. 在导航菜单（☰）上，单击**管理**。
2. 在**数据源**部分中的**流**下，单击**流源**。
3. 选择要删除的流源，然后单击**删除**。
4. 在**管理**选项卡上，单击**部署更改**。

流源别名

流源别名使用虚拟名称来标识发送到流收集器上的相同端口的外部流。例如，IBM QRadar QFlow Collector 可具有侦听端口 2055 的单个 NetFlow 流源，并且具有发送到相同 QRadar QFlow Collector 的多个 NetFlow 源。通过使用流源别名，您可以基于其 IP 地址标识不同的 NetFlow 源。

在 QRadar QFlow Collector 接收来自具有 IP 地址但是无当前别名的设备的流量时，QRadar QFlow Collector 尝试逆向 DNS 查找。查找用于确定设备的主机名。

您可以配置 QRadar QFlow Collector 以自动创建流源别名。在 QRadar QFlow Collector 收到来自具有 IP 地址但无当前别名的设备的流量时，其执行逆向 DNS 查找以确定设备的主机名。

如果查找成功，那么 QRadar QFlow Collector 将此信息添加到数据库并向环境中的所有 QRadar QFlow Collector 组件报告此信息。如果查找失败，那么 QRadar 基于流源名称和源 IP 地址为流源创建缺省别名。例如，缺省别名可能显示为 **default_NetFlow_172.16.10.139**。

添加流源别名

使用“**流源别名**”窗口可添加流源别名。

过程

1. 在导航菜单（☰）上，单击**管理**。
2. 在**数据源**部分中的**流**下，单击**流源别名**。
3. 执行下列其中一项操作：
   - 要添加流源别名，请单击**添加**并输入各参数的值。
   - 要编辑现有的流源别名，请选择流源别名，单击**编辑**，然后更新参数。
4. 单击**保存**。
5. 在**管理**选项卡上，单击**部署更改**。

注： 如果将流源别名重命名，那么必须使用原始名称来执行历史搜索。

删除流源别名

使用“**流源别名**”窗口删除流源别名。

过程

1. 在导航菜单（☰）上，单击**管理**。
2. 在**数据源**部分中的**流**下，单击**流源别名**。
3. 选择要删除的流源别名，然后单击**删除**。
4. 在**管理**选项卡菜单上，单击**部署更改**。

第 11 章 远程网络和服务配置

使用远程网络和服务组来表示特定概要文件的网络上的流量活动。远程网络组显示指定的远程网络上产生的用户流量。

所有远程网络和服务组都具有组级别和叶对象级别。通过将对象添加到现有组或更改先前的属性以适应环境，您可以编辑远程网络和服务组。

如果将现有对象移动到其他组，那么现有组中的对象名称将移动到新选择的组。但在部署配置更改后，存储在数据库中的对象数据将丢失且该对象将失去作用。要解决此问题，请新建一个视图并重新创建可与其他组共存的对象。

您可对远程网络和服务加以分组，以便用于定制规则引擎、流和事件搜索中。您还可在 IBM QRadar Risk Manager（如果可用）中对网络和服务进行分组。

相关概念

IBM QRadar 产品中的功能

缺省远程网络组

IBM QRadar 包含缺省远程网络组。

下表描述了缺省远程网络组。

表 *26.* 缺省远程网络组

组	描述
BOT	指定源自 BOT 应用程序的流量。 有关更多信息，请参阅 Botnet Command and Control drop rules on the Emerging Threats Web 站点 (http://rules.emergingthreats.net/blockrules/emerging-botcc.rules)
Bogon	指定源自未分配的 IP 地址的流量。 有关更多信息，请参阅 Team CYMRU Web 站点上有关 bogon 的参考资料 (http://www.team-cymru.org/Services/Bogons/bogon-bn-nonagg.txt)。
HostileNets	指定源自已知有害网络的流量。 HostileNets 有一组 20（按 1 - 20（含）排列）个可配置的 CIDR 范围。 有关更多信息，请参阅 DShield Web 站点上有关 HostileNets 的参考资料 (http://www.dshield.org/ipsascii.html?limit=20)
近邻	指定源自附近网络的流量，您的组织与这些附近网络具有网络同级协议。 该组缺省情况下为空。您必须配置该组以对来自近邻网络的流量进行分类。
Smurfs	指定源自 smurf 攻击的流量。 smurf 攻击是一种拒绝服务攻击，通过欺骗性广播 ping 消息来冲击目标系统。

表 26. 缺省远程网络组 (续)	
组	**描述**
Superflows	该组不可配置。 活动流是聚集具有一组相似预定义元素的多个流而形成的流。
TrustedNetworks	指定来自可信网络的流量，此类可信网络包括具有对关键应用程序和服务的远程访问权的业务合作伙伴。 该组缺省情况下为空。 您必须配置该组以对来自可信网络的流量进行分类。
监测列表	对源自要监视的网络的流量进行分类。 该组缺省情况下为空。

包含活动流的组和对象仅供参考，无法编辑。包含 Bogon 的组和对象可通过自动更新功能来进行配置。

注: 您可以使用参考集代替远程网络以提供其中部分功能。虽然可以向参考表中的 IP 值分配置信度级别，但参考集仅用于单一 IP，无法配合 CIDR 范围使用。远程网络更新后，您可以使用 CIDR 值，但不能配合权重或置信度级别使用。

相关概念

第 73 页的『参考数据集合的类型』

存在不同类型的参考数据集合，每种类型可处理不同级别的数据复杂性。最常用类型是参考集和参考映射。

缺省远程服务组

IBM QRadar 包含缺省远程服务组。

下表描述了缺省远程服务组。

表 27. 缺省远程网络组	
参数	**描述**
IRC_Servers	指定源自俗称交谈服务器的地址的流量。
Online_Services	指定源自俗称联机服务的地址的流量，此类服务可能涉及数据丢失。
Porn	指定源自俗称包含显式色情材料的地址的流量。
Proxies	指定源自俗称开放式代理服务器的流量。
Reserved_IP_ Ranges	指定源自保留的 IP 地址范围的流量。
Spam	指定源自俗称用于生成垃圾邮件或不需要的电子邮件的地址的流量。
Spy_Adware	指定源自俗称包含间谍软件或广告软件的地址流量。
Superflows	指定源自俗称用于生成活动流的流量。
Warez	指定源自俗称包含盗版软件的地址的流量。

网络资源准则

鉴于大型结构网络中 IBM QRadar SIEM 所需应对的复杂状况以及网络资源需求，请遵循建议的准则进行操作。

下表描述了可供您遵循的部分建议实践：

- 捆绑对象，并使用**网络活动**和**日志活动**选项卡来对网络数据进行分析。

  对象越少，对磁盘造成的输入和输出也越少。

- 通常对于标准系统需求，请勿超出每个组 200 个对象。

  更多对象可能会影响调查流量时的处理能力。

管理远程网络对象

创建远程网络组之后，您可以按远程网络组汇总流和事件搜索结果。您还可以创建按远程网络组来测试活动的规则。

使用“**远程网络**”窗口可以添加或编辑远程网络对象。

过程

1. 在导航菜单（☰）上，单击**管理**。
2. 在**远程网络和服务配置**部分中，单击**远程网络和服务**。
3. 要添加远程网络对象，请单击**添加**并输入各参数的值。
4. 要编辑远程网络对象，请完成下列步骤：
   a) 双击组名。
   b) 选择概要文件并单击编辑图标 (✎) 以编辑远程概要文件。
5. 单击**保存**。
6. 单击“上一步”图标 (❮) 以返回到“**远程网络和服务**”窗口。
7. 在**管理**选项卡上，单击**部署更改**。

管理远程服务对象

远程服务组对源自用户定义的网络范围或 IBM 自动更新服务器的流量进行组织。创建远程服务组之后，您可以汇总流和事件搜索结果，以及创建按远程服务组来测试活动的规则。

使用“**远程服务**”窗口可以添加或编辑远程服务对象。

过程

1. 在导航菜单（☰）上，单击**管理**。
2. 在**远程网络和服务配置**部分中，单击**远程网络和服务**。
3. 要添加远程服务对象，请单击**添加**并输入参数值。
4. 要编辑远程服务对象，请单击要显示的组，再单击**编辑**图标，然后更改值。
5. 单击**保存**。
6. 单击**返回**。
7. 关闭“**远程服务**”窗口。
8. 在**管理**选项卡菜单上，单击**部署更改**。

第 12 章 服务器发现

服务器发现功能使用“资产概要文件”数据库来发现基于端口定义的不同服务器类型。然后，您可以针对规则选择服务器以添加到服务器类型构建块。

服务器发现功能基于服务器类型构建块。使用端口定义服务器类型。因此，在搜索“资产概要文件”数据库时，服务器类型构建块的运行方式与基于端口的过滤器相同。

有关构建块的更多信息，请参阅 *IBM QRadar User Guide*。

使用**服务器发现**功能和 IBM QRadar Vulnerability Manager 以针对良性漏洞常见例外规则。减少针对以下**服务器类型**看到的漏洞数量：

表 *28.* 服务器类型漏洞

服务器类型	**漏洞**
FTP 服务器	**存在 FTP 服务器**
DNS 服务器	**DNS 服务器正在运行**
邮件服务器	**检测到 SMTP 服务器**
Web 服务器	**Web Service 正在运行**

有关误报漏洞的更多信息，请参阅《*IBM QRadar Vulnerability Manager* 用户指南》。

相关概念

IBM QRadar 产品中的功能

发现服务器

使用**资产**选项卡以发现网络上的服务器。

过程

1. 在导航菜单 (☰) 上，单击**资产**以打开**资产**选项卡。
2. 在**资产**导航菜单上，单击**服务器发现**。
3. 从**服务器类型**列表，选择要发现的服务器类型。
4. 选择以下其中一个选项以确定要发现的服务器：
   - 要使用当前所选的**服务器类型**以搜索部署中的所有服务器，请选择**所有**。
   - 要搜索部署中分配给当前所选**服务器类型**的服务器，请选择**已分配**。
   - 要搜索部署中未分配的服务器，请选择**未分配**。
5. 要编辑标准服务器端口列表，请单击**编辑端口**。
6. 从**网络**列表，选择要搜索的网络。
7. 单击**发现服务器**。
8. 在**匹配服务器**表中，选中要分配给服务器角色的所有服务器的复选框。
9. 单击**批准选定的服务器**。

第 13 章 域分段

将网络分段到多个不同的域中，以帮助确保相关信息仅可供需要此类信息的用户使用。

您可创建安全概要文件以限制可供该域中的用户组可用的信息。安全概要文件仅为授权用户提供了针对完成其日常任务所需的信息的访问权。您只能修改受影响的用户的安全概要文件，不能单独修改每个用户。

您还可以使用域来管理重叠的 IP 地址范围。使用共享 IBM QRadar 基础结构从多个网络收集数据时，此方法很有用。通过创建表示网络上特定地址空间的域，可使位于各独立域中的多个设备具有相同的 IP 地址，但仍可作为独立设备来处理。

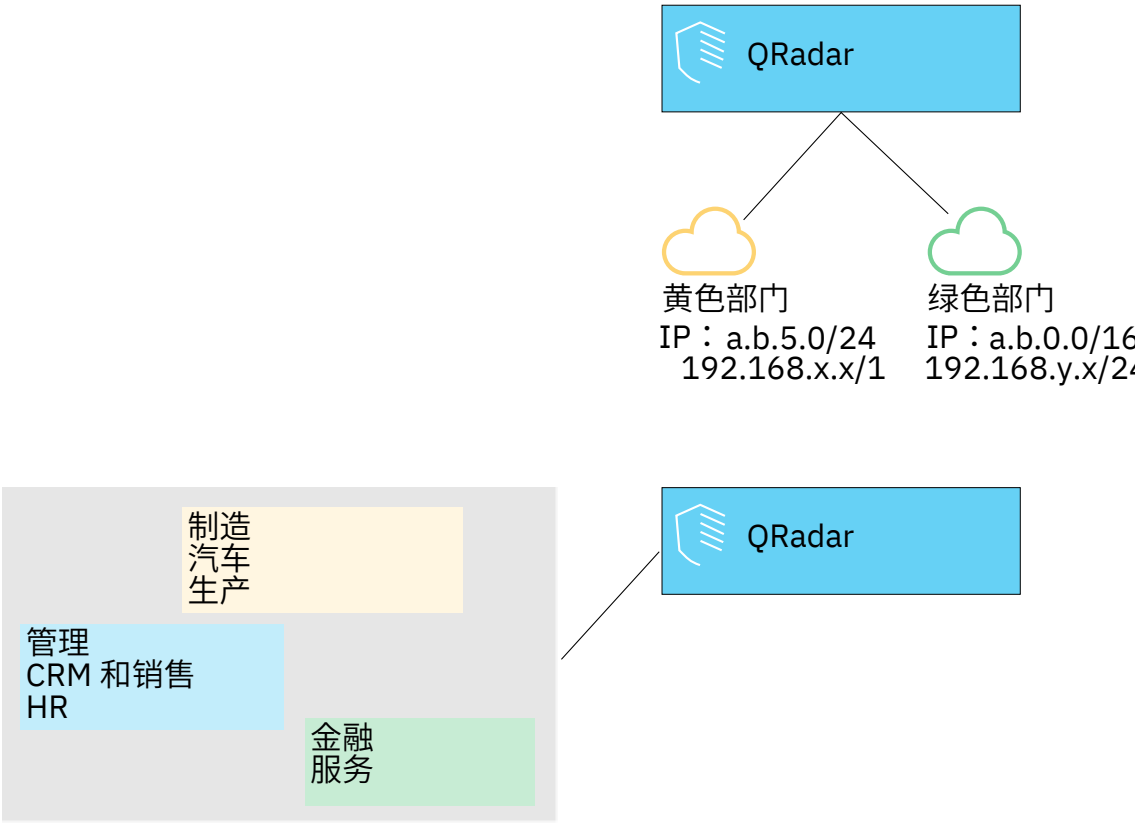

图 9. 域分段

相关概念

IBM QRadar 产品中的功能

重叠 IP 地址

重叠 IP 地址即分配给网络上的多个设备或逻辑单元（例如，事件源类型）的 IP 地址。重叠的 IP 地址范围可能导致企业收购后合并网络时出现重大问题或者给带来新客户的受管安全服务供应商 (MSSP) 造成重大问题。

IBM QRadar 必须能够区分来自不同设备且具有相同 IP 地址的事件和流。如果将相同 IP 地址分配给多个事件源，可以创建域来对其加以区分。

例如，假设以下情况，公司 A 收购公司 B，并且想要使用 QRadar 的共享实例来监视新公司的资产。收购具有类似的网络结构，导致对每家公司内不同日志源使用相同 IP 地址。具有相同 IP 地址的日志源可能导致关联、报告、搜索和资产概要分析方面出现问题。

要区分从日志源进入 QRadar 的事件和流的来源，可以创建两个域，并将每个日志源分配到不同的域。如果需要，还可以将每个事件收集器、流收集器或数据网关分配到与向其发送事件的日志源所在的域中。

要查看由域传入的事件，请创建搜索并在搜索结果中包含域信息。

域定义和标记

基于 IBM QRadar 输入源对域进行定义。当事件和流进入 QRadar 时，将对域定义进行评估，并使用域信息对事件和和流进行标记。

指定事件的域

下图显示评估事件的域条件的优先顺序。

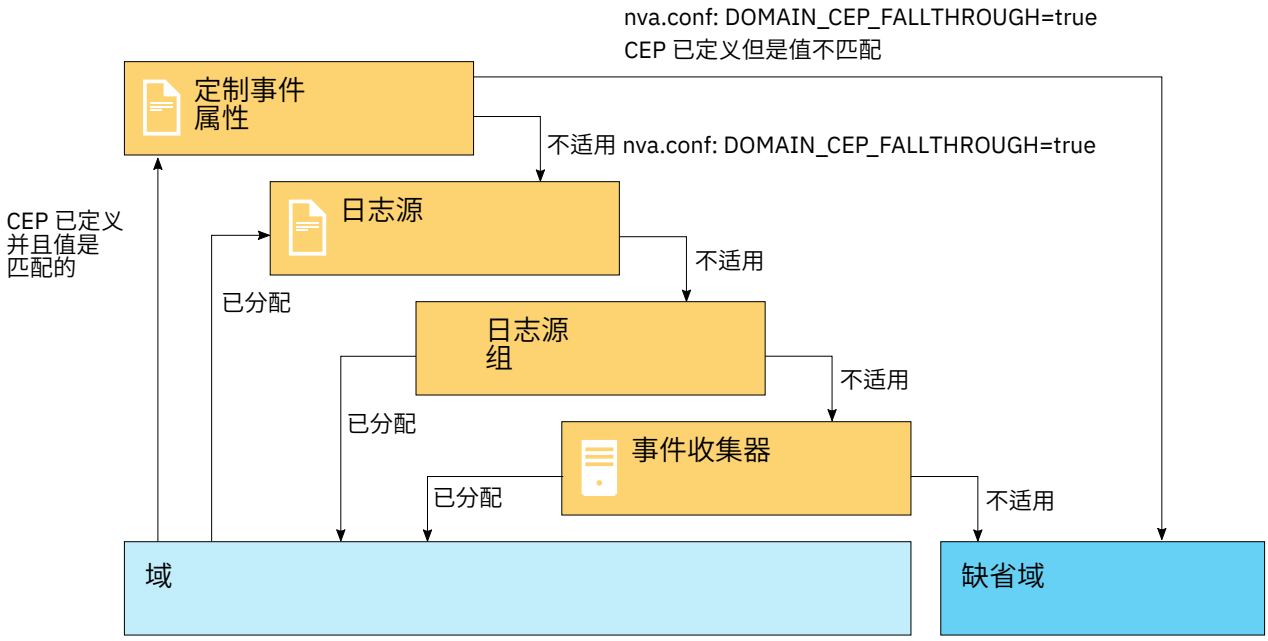

图 *10.* 事件的优先顺序

以下是指定事件域的方法：

事件收集器和数据网关

如果将事件收集器或数据网关专用于特定网段或 IP 地址范围，那么可以将整个事件收集器或数据网关标记为该域的一部分。

到达该事件收集器或数据网关的所有日志源都属于该域；因此，任何新的自动检测到的日志源将自动添加到该域中。

要点:

如果将事件源从一个事件收集器或数据网关重定向到不同域中的另一个，必须通过以下一种方式更新其日志源：

· 编辑日志源以更新事件收集器或数据网关信息。

· 删除日志源并部署完整配置，从而在新事件收集器或数据网关上自动删除事件源。

除非更新日志源，否则具有域限制的非管理用户可能看不到与日志源相关联的攻击。

日志源

您可以将特定日志源配置为属于某个域。

对于事件收集器或数据网关可以从多个域接收事件的部署，此标记域的方法是一个选项。

日志源组

您可以将日志源组分配给特定域。此选项允许对日志源配置进行更广泛的控制。

添加到日志源组的任何新日志源都将自动获取与日志源组相关联的域标记。

定制属性

您可以将定制属性应用于来自日志源的日志消息。

要确定特定日志消息属于哪个域，请根据“域管理”编辑器中定义的映射来查找该定制属性的值。

此选项用于多地址范围或多租户日志源，例如文件服务器和文档存储库。

指定流的域

下图显示评估流的域条件的优先顺序。

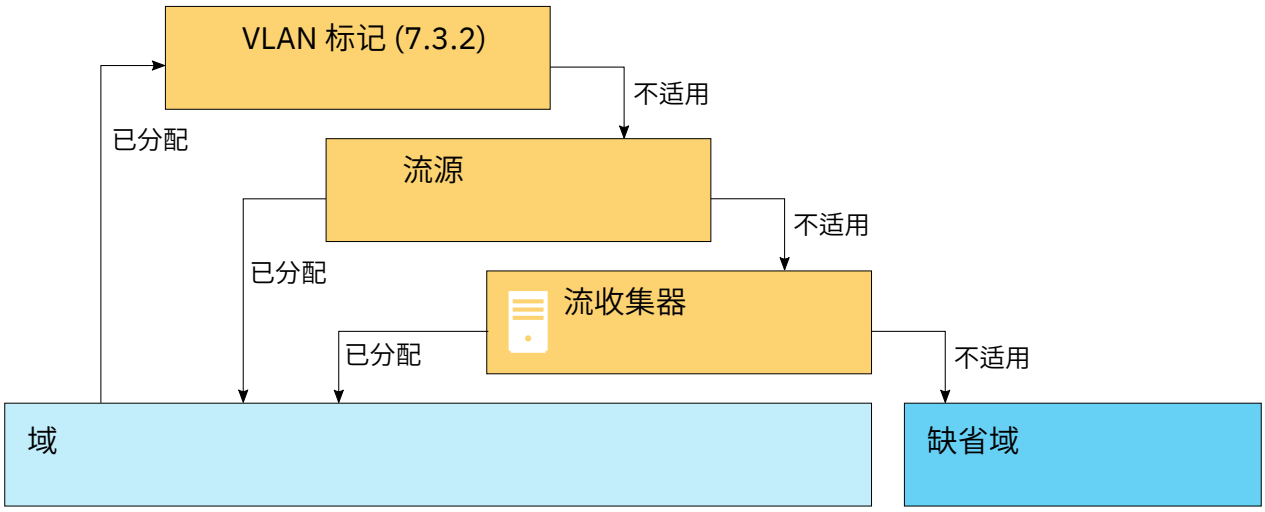

图 *11.* 流的优先顺序

以下是指定流的域的方法：

流收集器和数据网关

您可以将特定数据网关分配给域。

到达该流收集器或数据网关的所有流源都属于该域；因此，任何新的自动检测到的流源将自动添加到该域中。

流源

您可以将特定流源指定给域。

当单个 流收集器或数据网关正从多个网段或包含重叠 IP 地址范围的路由器中收集流时，此选项有用。

流 VLAN 标识

您可以将特定 VLAN 指定给域。

在从多个网段（通常包含重叠 IP 范围）收集流量时此选项非常有用。此 VLAN 定义基于企业和客户 VLAN 标识。

在分析包含 VLAN 信息的流时，将从 QFlow 发送以下信息元素。可在域定义中分配以下两个字段：

- PEN 2 (IBM)，元素标识 82：企业 VLAN 标识
- PEN 2 (IBM)，元素标识 83：客户 VLAN 标识

指定扫描结果的域

您还可以将漏洞扫描程序分配给特定域，以便将扫描结果正确标记为属于该域。域定义可包含所有 QRadar 输入源。

有关将网络分配给预配置域的更多信息，请参阅 第 33 页的『网络层次结构』。

评估域条件的优先顺序

当事件和流进入 QRadar 系统时，将基于域定义的详细程度对域条件进行评估。

如果域定义基于事件，那么首先针对映射到域定义的任何定制属性检查入局事件。如果定制属性中定义的正则表达式的结果与域映射不匹配，那么该事件将自动分配到缺省域。

如果事件与定制属性的域定义不匹配，那么将应用以下优先顺序：

1. 日志源
2. 日志源组
3. 事件收集器或数据网关

如果基于流对域进行定义，那么将应用以下优先顺序：

1. 流源
2. 流收集器或数据网关

如果扫描程序具有关联的域，那么扫描程序发现的所有资产将自动分配到扫描程序所在的域。

将数据转发到另一个 QRadar 系统

将数据转发到另一个 QRadar 系统时，将移除域信息。包含域信息的事件和流会自动分配到接收 QRadar 系统上的缺省域。要确定将哪些事件和流分配到缺省域，您可以在接收系统上创建定制搜索。您可能想要将这些事件和流重新分配到用户定义的域。

创建域

使用“**域管理**”窗口基于 IBM QRadar 输入源创建域。

关于此任务

创建域时，请遵循下列准则：

- 未分配给用户定义的域的所有项将自动分配给缺省域。具有有限域访问权的用户不应该具有管理特权，因为此特权会授予对所有域的不受限制访问权。
- 您可以将相同定制属性映射到两个不同的域，但是针对每个域，捕获结果必须不同。
- 无法将日志源、日志源组、事件收集器或数据网关分配给两个不同域。将日志源组分配给域时，每个映射的属性都在“**域管理**”窗口中显示。

必须使用关联的域更新安全概要文件。更新安全概要文件且部署更改后才会应用域级别限制。

过程

1. 在导航菜单（☰）上，单击**管理**。
2. 在**系统配置**部分中，单击**域管理**。
3. 要添加域，请单击**添加**，并为域输入唯一名称和描述。

   提示: 您可以通过在**输入域名**搜索框中输入名称，检查唯一名称。
4. 根据将定义的域条件，单击相应选项卡。
   - 要根据定制属性、日志源组、日志源、事件收集器或数据网关定义域，请单击**事件**选项卡。
   - 要根据流源定义域，请单击**流**选项卡。
   - 要根据扫描程序（包括 IBM QRadar Vulnerability Manager 扫描程序）定义域，请单击**扫描程序**选项卡。
5. 要将定制属性分配给域，请在**捕获结果**框中，输入与正则表达式 (regex) 过滤器的结果匹配的文本。

   要点: 必须在“**定制事件属性**”窗口中选中**规则、报告和搜索的定制解析**复选框，才能解析和存储定制事件属性。未选中此选项时，不会进行域分段。
6. 从列表选择域条件，并单击**添加**。
7. 将源项添加到域后，单击**创建**。

下一步做什么

创建安全概要文件，用于定义可访问域的用户。在环境中创建第一个域后，必须更新所有非管理用户的安全概要文件以指定域分配。在域感知环境中，对于安全概要文件未指定域分配的非管理用户，他们不会看到任何日志活动或网络活动。

查看网络的层次结构配置，并将现有 IP 地址分配给正确的域。有关更多信息，请参阅第 33 页的『网络层次结构』。

针对 VLAN 流创建域

使用“**域管理**”窗口以基于 IBM QRadar VLAN 流源创建域。

关于此任务

在 QRadar 中，可以根据流中包含的 VLAN 信息向传入流分配域。这些传入流将映射到包含相同 VLAN 定义的域。

过程

1. 在导航菜单（☰）上，单击**管理**。
2. 在**系统配置**部分中，单击**域管理**。
3. 单击**添加**，并输入域的唯一名称和描述。

   提示: 您可以通过在**输入域名**搜索框中输入名称，检查唯一名称。

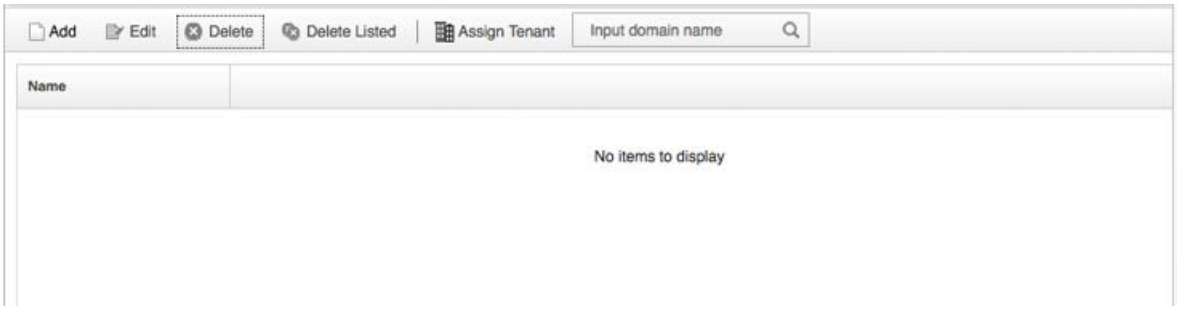

图 *12.* 输入域名

4. 单击**流**选项卡，然后选择**流 VLAN 标识**。
5. 选择匹配传入流上的值的“企业 VLAN 标识”和“客户 VLAN 标识”值，然后单击**添加**。

   注：

   · “企业 VLAN 标识 (IE)：82”由传入流上的“专用企业编号 (PEN)：2”信息元素 (IE) 指定。

   · “客户 VLAN 标识”由传入流上的“PEN：2”和“IE：83”指定。

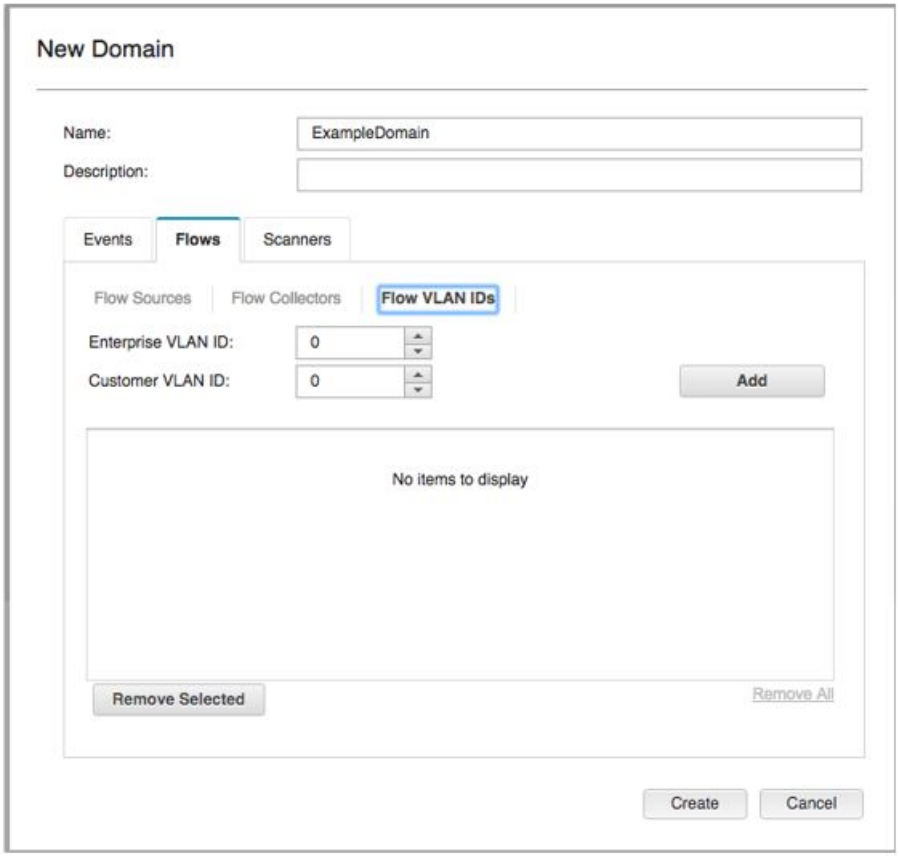

图 *13.* 新域

6. 在**名称**字段中，输入域的唯一名称，然后单击**创建**。

结果

这将创建域定义并映射传入流。域的租户分配照常发生。

图 *14.* 域定义已创建

从安全概要文件派生的域特权

您可使用安全概要文件来授予域特权，并确保在整个 IBM QRadar 系统中都遵循域限制。安全概要文件还可简化业务需求突然发生改变时大量用户的权限管理。

用户只能查看域边界范围内针对为其分配的安全概要文件所设置的数据。安全概要文件包含域作为首要条件之一，并通过评估此条件来限制对系统的访问。将域分配给安全概要文件时，它将优先于其他安全许可权。评估域限制后，将评估各安全概要文件以确定此特定概要文件的网络和日志许可权。

例如，如果为用户授予对 Domain_2 的特权和对网络 10.0.0.0/8 的访问权，那么该用户只能查看来自 Domain_2 并且包含来自 10.0.0.0/8 网络的事件、攻击、资产和流。

作为 QRadar 管理员，您可查看所有域，并且可向非管理用户分配域。请勿将管理特权分配给要限制于特定域的用户。

必须使用关联的域更新安全概要文件。在更新安全概要文件以及部署更改前，不会应用域级别限制。

向安全概要文件分配域时，可以授予对以下类型的域的访问权。

用户定义的域

可使用“域管理工具”基于输入源来创建域。有关更多信息，请参阅创建域。

缺省域

未分配给用户定义的域的所有一切都会自动分配给缺省域。缺省域包含系统范围的事件。

注: 有权访问缺省域的用户可以查看系统范围的事件，无任何限制。向用户分配缺省域访问权之前，请确保此访问权可接受。所有管理员都有权访问缺省域。

在共享的事件收集器或数据网关上自动发现的所有日志源（未显式分配给任何域的日志源）都会在缺省域上被自动发现。这些日志源需要手动干预。要识别这些日志源，必须定期在按日志源分组的缺省域中运行搜索。

所有域

如果分配给用户的安全概要文件具有针对**所有域**的访问权，那么此类用户可查看系统中的所有活动域、缺省域和原先在整个系统中已删除的任何域。他们还可查看将来创建的所有域。

无法将已删除的域分配到安全概要文件。如果用户具有**所有域**分配，或者如果域被删除前已分配给用户，那么在针对事件、流、资产和攻击的历史搜索结果中会返回已删除的域。运行搜索时无法按已删除的域进行过滤。

管理用户可以在“**域管理**”窗口的**汇总**选项卡上查看已分配给安全概要文件的域。

域感知环境内的规则修改

同时具备**维护定制规则**和**查看定制规则**许可权的任何用户均可查看、修改或禁用规则，与用户所属的域无关。

要点: 向用户角色添加**日志活动**功能时，会自动授予**维护定制规则**和**查看定制规则**许可权。具有这些许可权的用户可以访问所有域的所有日志数据，并且可编辑所有域中的规则，即使其安全概要文件设置具有域级别的限制也是如此。要防止用户访问其他域中的日志数据和修改规则，请编辑用户角色，并移除**维护定制规则**和**查看定制规则**许可权。

域感知搜索

您可使用域作为定制搜索中的搜索条件。您的安全概要文件可控制可供您搜索的域。

系统范围的事件和未分配给用户定义的域的事件将自动分配给缺省域。管理员或具有提供对缺省域的访问权的安全概要文件的用户可以创建定制搜索以查看未分配给用户定义的域的所有事件。

缺省域管理员可以与其他域用户共享已保存的搜索。当域用户运行该已保存的搜索时，搜索结果将限制于其域内。

特定于域的规则和攻击

规则可在单一域的上下文中或者在所有域的上下文中运行。域感知规则提供了包含**并且域为**测试的选项。

下图显示使用多个域的示例。

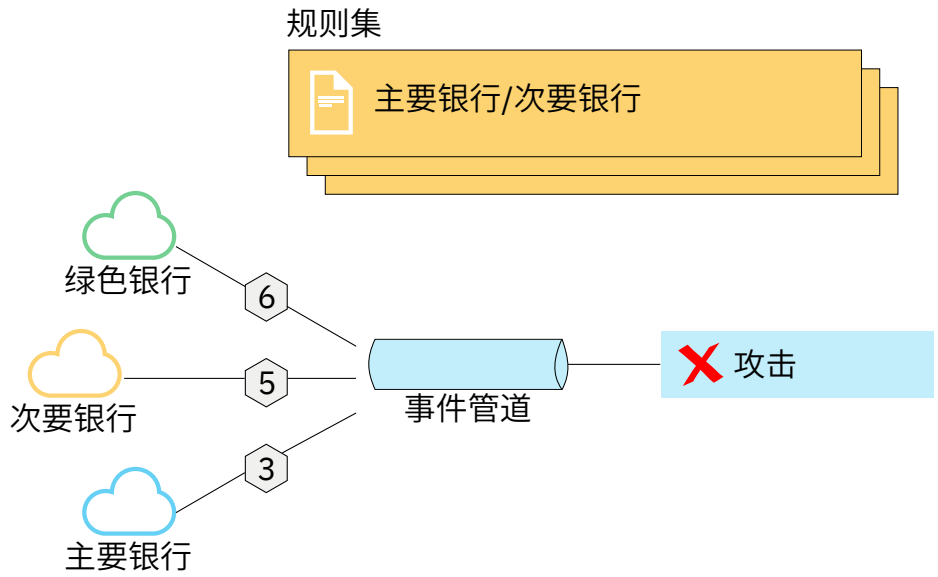

图 *15.* 域感知规则

您可限制规则以使其仅适用于指定域内发生的事件。如果事件包含的域标记不同于规则上设置的域，那么此事件不会触发事件响应。

在不具有用户定义的域的 IBM QRadar 系统中，每次触发规则时，规则会创建攻击并保持对其施加影响。在域感知环境中，每次在不同域的上下文中触发规则时，规则都会创建新的攻击。

在所有域的上下文中运行的规则都被称为系统范围的规则。要创建系统范围的规则以测试整个系统的条件，请针对**并且域为**测试选择域列表中的**任何域**。**任何域**规则会创建**任何域**攻击。

单域规则
如果规则为有状态的规则，那么会为每个域单独保留状态。单独为每个域触发规则。触发规则时，会为所涉及的每个域单独创建攻击，并且以这些域来标记攻击。

单域攻击
以对应域名来标记攻击。它仅包含以该域标记的事件。

系统范围规则
如果规则为有状态的规则，那么会为整个系统保留单一状态，并忽略域标记。当规则运行时，它会创建会影响单一系统范围攻击。

系统范围攻击
以**任何域**标记攻击。它仅包含以所有域标记的事件。

下表提供了域感知规则的示例。此示例使用定义有三个域的系统：Domain_A、Domain_B 和 Domain_C。

下表中的规则示例可能不适用于您的 QRadar 环境。例如，使用流和攻击的规则不适用于 IBM QRadar Log Manager。

表 *29.* 域感知规则

域文本	说明	规则响应
以下域之一：Domain_A	仅查找以 Domain_A 标记的事件，并忽略以其他域标记的规则。	创建或影响以 Domain_A 标记的攻击。
以下域之一：Domain_A，并且定义为**在 1 分钟内检测到 10 次 HTTP 流**的有状态的测试	仅查找以 Domain_A 标记的事件，并忽略以其他域标记的规则。	创建或影响以 Domain_A 标记的攻击。为 Domain_A 保留单一状态的 HTTP 流计数器。

表 29. 域感知规则 (续)

域文本	说明	规则响应
以下域之一：Domain_A 或 Domain_B	仅查找以 Domain_A 和 Domain_B 标记的事件，并忽略以 Domain_C 标记的事件。 此规则充当单一域规则的两个独立实例，并为不同域创建独立攻击。	对于以 Domain_A 标记的数据，它会创建或影响以 Domain_A 标记的单一域攻击。 对于以 Domain_B 标记的数据，它会创建或影响以 Domain_B 标记的单一域攻击。
以下域之一：Domain_A 或 Domain_B，并且定义为**在 1 分钟内检测到 10 次 HTTP 流**的有状态的测试	仅查找以 Domain_A 和 Domain_B 标记的事件，并忽略以 Domain_C 标记的事件。 此规则充当单一域规则的两个独立实例，并为两个不同域保留两个独立状态（HTTP 流计数器）。	当规则在一分钟内检测到以 Domain_A 标记的 10 个 HTTP 流时，它会创建或影响以 Domain_A 标记的攻击。 当规则在一分钟内检测到以 Domain_B 标记的 10 个 HTTP 流时，它会创建或影响以 Domain_B 标记的攻击。
未定义任何域测试	查找以所有域标记的事件，并按每个域创建或影响攻击。	每个独立域都具有为其生成的攻击，但攻击不包含来自其他域的影响。
规则具有定义为**在 1 分钟内检测到 10 次 HTTP 流**的有状态的测试，并且未定义任何域测试	查找以 Domain_A、Domain_B 或 Domain_C 标记的事件。	为每个与保留独立状态并创建独立攻击。
以下域之一：任何域	查找所有事件，与标记的域无关。	创建或影响以任何域标记的单一系统范围攻击。
以下域之一：任何域，并且定义为**在 1 分钟内检测到 10 次 HTTP 流**的有状态的测试	查找所有事件，与标记的域无关，并且为所有域保留单一状态。	创建或影响以任何域标记的单一系统范围攻击。 例如，如果在 1 分钟内检测到 3 个以 Domain_A 标记的域、3 个以 Domain_B 标记的事件和 4 个以 Domain_C 标记的事件，那么它会创建一次攻击，因为总计检测到 10 个事件。
以下域之一：任何域或 Domain_A	与具有**以下域之一：任何域**的规则的运行方式相同。	当域测试包含任何域时，会忽略列出的任何单一域。

查看攻击表时，可单击**域**列以对攻击进行排序。排序功能中不包含**缺省域**，因此它不包含在按字母顺序显示的排序中。但根据列按升序还是降序排序，它会显示在**域**列表顶部或底部。**任何域**不会显示在攻击列表中。

示例：基于定制属性的域特权分配

如果日志文件包含要在域定义中使用的信息，那么可将此类信息作为定制事件属性予以公开。

基于捕获结果向域分配定制属性。可向多个域分配相同定制属性，但捕获结果必须不同。

例如，定制事件属性（如 userID）可通过求值生成单一用户或用户列表。每个用户都只能属于一个域。

在下图中，日志源包含作为定制属性 userID 公开的用户标识信息。事件收集器或数据网关会返回两个用户文件，并且每个用户仅分配到一个域。在此案例中，一个用户分配到域：9，另一个用户分配到域：12。

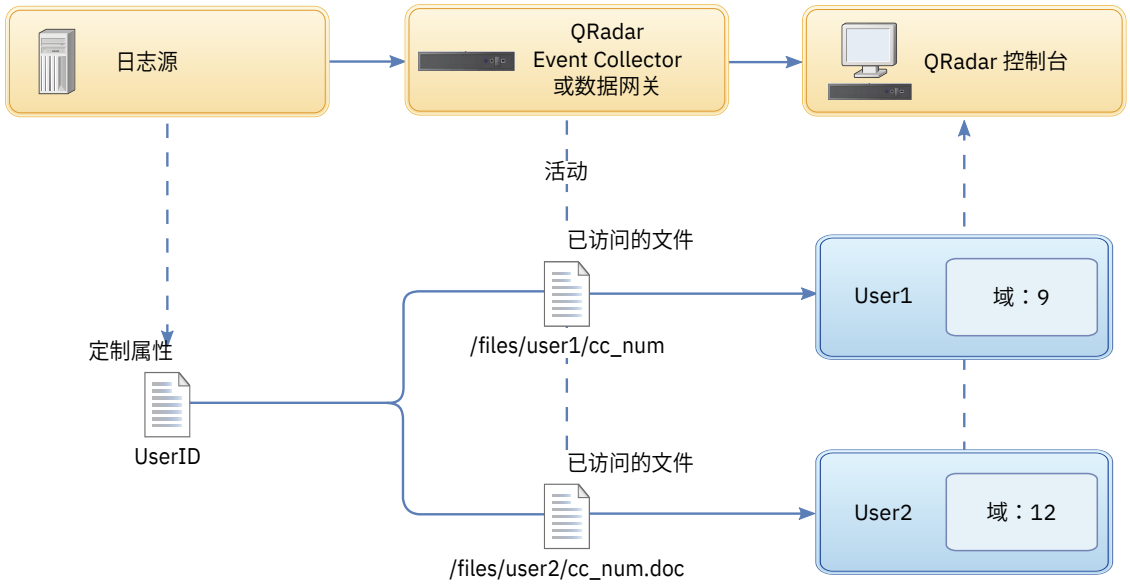

图 *16.* 使用定制事件属性分配域

如果捕获结果返回的用户未分配到用户定义的特定域，那么会将该用户自动分配到缺省域。缺省域分配需要手动干预。请执行定期搜索以确保缺省域中的所有实体均已正确分配。

要点: 在域定义中使用定制属性前，请确保已选中**定制事件属性**窗口上的**针对规则、报告和搜索优化解析**。该选项可确保 IBM QRadar 首次收到事件时会对定制事件属性进行解析和存储。如果未选中该选项，那么不会发生域分段。

第 14 章 多租户管理

多租户环境允许安全管理服务供应商 (MSSP) 和多部门组织从单个共享的 IBM QRadar 环境向多个客户组织提供安全服务。您不必针对每个客户部署一个唯一的 QRadar 实例。

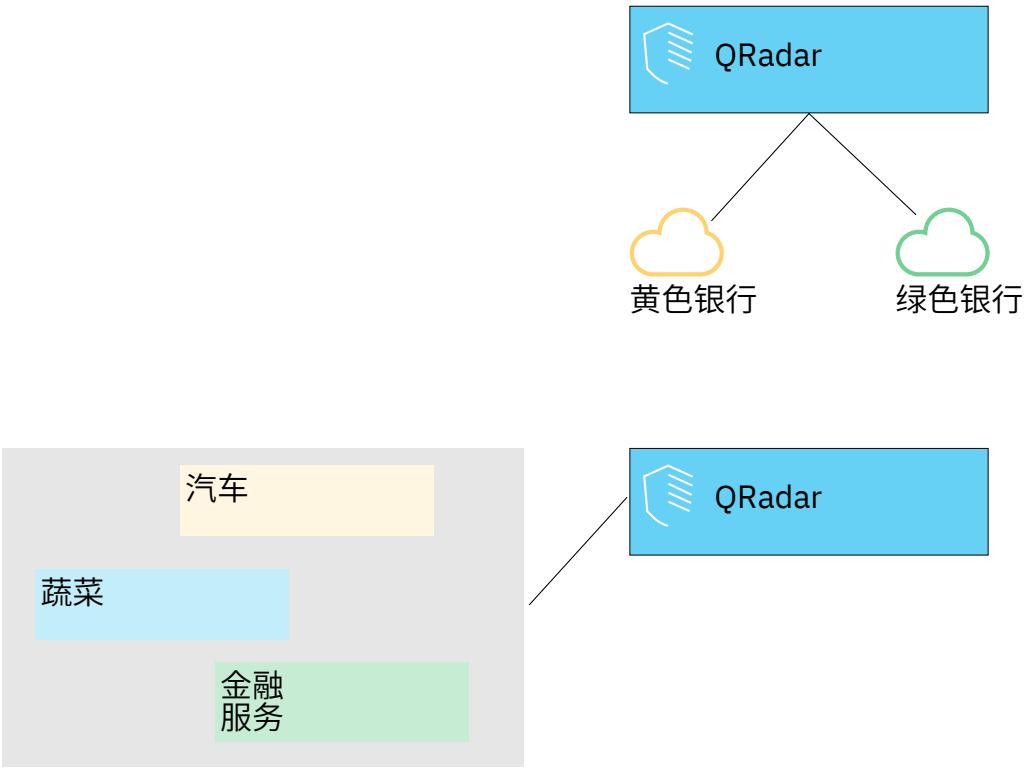

图 *17.* 多租户环境

在多租户部署中，通过创建基于 QRadar 输入源的域，确保客户只能看到自己的数据。然后，使用安全概要文件和用户角色来管理域中大型用户组的特权。安全概要文件和用户角色确保用户只能访问授权其使用的信息。

相关概念

IBM QRadar 产品中的功能

多租户环境中的用户角色

多租户环境包含服务提供者和多个租户。每个角色具有不同的职责和关联的活动。

服务提供者

服务提供者拥有系统并按多个租户管理系统使用。服务提供者可查看所有租户的数据。安全管理服务供应商 (MSSP) 管理员通常负责以下活动：

- 管理和监视 IBM QRadar 部署的系统运行状况。
- 供应新租户。
- 针对租户管理员和用户创建角色和安全概要文件。
- 保护系统远离未经授权的访问。
- 创建域以隔离租户数据。
- 部署租户管理员在租户环境中执行的更改。
- 监视 QRadar 许可证。

· 与租户管理员协作。

租户

每个租赁都包含租户管理员和租户用户。租户管理员可以是租户组织的员工，或者服务提供者可代表客户管理租户。

租户管理员负责以下活动：

· 配置其自己的租赁中的网络层次结构定义。

· 配置和管理租户数据。

· 查看日志源。可编辑日志源以合并数据并可禁用日志源。

· 与 MSSP 管理员协作。

租户管理员可以配置特定于租户的部署，但是无法访问或更改其他租户的配置。他们必须联系 MSSP 管理员以在 QRadar 环境中部署更改，包括自己的租户中的网络层次结构更改。

租户用户无管理特权并且只能查看其有权访问的数据。例如，用户可能仅有权查看包含多个日志源的域中 1 个日志源的数据。

多租户环境中的域和日志源

使用域来分隔重叠的 IP 地址，并将单个数据源（例如，事件和流）分配到特定于租户的数据集。

在事件或流进入 IBM QRadar 时，QRadar 评估配置的域定义，并将事件和流分配给域。一个租户可以有多个域。如果未指定域，那么会将事件和流分配给缺省域。

域分段

域是用于根据数据源分隔数据虚拟存储区。它们是针对多租户环境的构建块。从以下输入源配置域：

· 事件和流收集器

· 流源

· 日志源和日志源组

· 定制属性

· 扫描程序

多租户部署可能由基本硬件配置组成，其中包含一个 QRadar 控制台、一个中央事件处理器以及每个客户一个事件收集器。在此配置中，在收集器级别定义域，然后将 QRadar 收到的数据自动分配给域。

要进一步整合硬件配置，您可以将一个收集器用于多个客户。如果日志或流源由相同数据收集器进行汇总但是属于不同租户，那么可将源分配给不同域。在日志源级别使用域定义时，每个日志源名称在整个 QRadar 部署中必须唯一。

如果需要分隔来自单个日志源的数据并将其分配给不同域，那么可从定制属性配置域。QRadar 查找有效内容中的定制属性，并将其分配给正确的域。例如，如果配置 QRadar 以与 Check Point Provider-1 设备相集成，那么可以使用定制属性以将来自此日志源的数据分配给不同的域。

自动日志源检测

在收集器级别定义域并且将专用事件收集器分配给单个域时，会将自动检测的新日志源分配给此域。例如，会将在 `Event_Collector_1` 上检测的所有日志源分配给 `Domain_A`。将在 `Event_Collector_2` 上自动收集的所有日志源分配给 `Domain_B`。

在日志源或定制属性级别定义域时，会自动将自动检测但尚未分配给域的日志源分配给缺省域。MSSP 管理员必须查看缺省域中的日志源并将它们分配给正确的客户机域。在多租户环境中，将日志源分配给特定域可避免数据泄露并在域上实施数据分隔。

供应新租户

作为安全管理服务提供商 (MSSP) 管理员，使用 IBM QRadar 的单个实例来为多个客户提供一个统一的体系结构，从而进行威胁检测和划分优先级。

在此场景中，您将加入新客户。供应新租户并创建租户管理员帐户（具有其自己的租户中的有限管理职责）。限制租户管理员的访问权，从而使他们无法查看或编辑其他租户中的信息。

在供应新租户之前，必须针对客户创建数据源，例如，日志源或流收集器，并将它们分配给域。

通过使用**管理**选项卡上的工具，完成以下任务以在 QRadar 中供应新租户：

1. 要创建租户，请单击**租户管理**。

   有关设置每个租户的每秒事件数 (EPS) 和每分钟流数 (FPM) 限制的信息，请参阅第 115 页的『监视多租户环境中的许可证使用情况』。
2. 要将域分配给租户，请单击**域管理**。
3. 要创建租户管理员角色并授予**代理管理**许可权，请单击**用户角色**。

   在多租户环境中，具有**代理管理**许可权的租户用户只能看到其自己的租户环境的数据。如果分配不属于**代理管理**的其他管理许可权，那么访问不再限制为此域。
4. 要通过指定租户域创建租户安全概要文件和限制数据访问，请单击**安全概要文件**。
5. 要创建租户用户并分配用户角色、安全概要文件和租户，请单击**用户**。

监视多租户环境中的许可证使用情况

作为安全管理服务提供商 (MSSP) 管理员，监视整个 IBM QRadar 部署上的事件和流速率。

在创建租户时，您可以设置每秒事件数 (EPS) 和每分钟流数 (FPM) 的限制。通过为每个租户设置 EPS 和 FPM 限制，您可以更好地管理多个客户机上的许可证容量。如果具有收集单个客户的事件或流的处理器，那么无需分配租户 EPS 和 FPM 限制。如果有单个处理器收集多个客户的事件或流，那么可为每个租户设置 EPS 和 FPM 限制。

如果将 EPS 和 FPM 限制设置为超过软件许可证或设备软件限制的值，那么系统自动针对此租户调速事件和流以确保不超过限制。如果未针对租户设置 EPS 和 FPM 限制，那么每个租户接收事件和流直至到达许可证限制或设备限制。许可限制应用于受管主机。如果经常超过许可证限制，那么可获取更适合部署的不同许可证。

查看每个日志源的 EPS 速率

使用**高级搜索**字段以输入 Ariel 查询语言 (AQL) 查询来查看日志源的 EPS 速率。

1. 在**日志活动**选项卡上，从**搜索**工具栏上的列表中选择**高级搜索**。
2. 要查看每个日志源的 EPS，在**高级搜索**字段中输入以下 AQL 查询：

```
select logsourcename(logsourceid) as LogSource, sum(eventcount) / 24*60*60 as EPS from events
group by logsourceid order by EPS desc last 24 hours
```

查看每个域的 EPS 速率

使用**高级搜索**字段以输入 Ariel 查询语言 (AQL) 查询来查看域的 EPS 速率。

1. 在**日志活动**选项卡上，从**搜索**工具栏上的下拉列表框中选择**高级搜索**。
2. 要查看每个域的 EPS，在**高级搜索**字段中输入以下 AQL 查询：

```
select DOMAINNAME(domainid) as LogSource, sum(eventcount) / 24*60*60 as EPS from events
group by domainid order by EPS desc last 24 hours
```

如果支想要查看日志源的平均 EPS 速率，那么单击**管理**选项卡上**数据源**窗格中的**日志源**。您可以使用此选项来快速标识日志源报告失败的配置问题。

多租户部署中的规则管理

在多租户环境中，必须定制规则以实现租户感知。 租户感知规则使用 **when the domain is one of the following** 规则测试，但是域修饰符确定规则的作用域。

下表显示如何使用域修饰符来更改多租户环境中规则的作用域。

表 *30.* 多租户环境中规则的作用域

规则作用域	**描述**	**规则测试示例**
单个域规则	这些规则仅包含 1 个域修饰符。	**and when the domain is one of the following:** *manufacturing*
单个租户规则	这些规则包含分配给租户的所有域。使用单个租户规则以关联单个租户中所有域的事件。	**and when the domain is one of the following:** *manufacturing, finance, legal*
全局规则	这些规则使用 **Any domain** 修饰符并在所有租户上运行。	**and when the domain is one of the following:***Any domain*

通过实现域感知，定制规则引擎 (CRE) 使用其各自的域自动隔离不同租户的事件相关性。有关在域分段网络中使用规则的更多信息，请参阅第 103 页的『第 13 章 域分段』。

多租户部署中的网络层次结构更新

IBM QRadar 使用网络层次结构来了解和分析环境中的网络流量。 具有**定义网络层次结构**许可权的租户管理员可更改自己的租户中的网络层次结构。

网络层次结构更改需要完整配置部署以在 QRadar 环境中应用更新。完整配置部署重新启动所有 QRadar 服务，并且事件和流的数据收集将停止直至部署完成。租户管理员必须联系安全管理服务提供商 (MSSP) 管理员来部署更改。MSSP 管理员可以在调度的停运期间规划部署，并提前通知所有租户管理员。

在多租户环境中，网络项目名称必须在整个部署中唯一。您无法使用具有相同名称的网络对象，即使将它们分配给不同的域。

相关概念

网络层次结构

IBM QRadar 使用网络层次结构对象和组来查看网络中的网络活动以及监视组或服务。

第 15 章 资产管理

为网络中的服务器和主机创建的资产和资产概要文件提供重要信息来帮助您解决安全问题。使用资产数据，您可以将系统中触发的攻击连接到物理或虚拟资产，从而提供安全性调查中的起点。

IBM QRadar 中的**资产**选项卡提供有关网络中资产的已知信息的统一视图。随着 QRadar 发现更多信息，系统会更新资产概要文件并以递增方式构建有关资产的完整概况。

系统根据从事件或流数据中被动吸收的身份信息或从 QRadar 在漏洞扫描期间主动查找的数据来动态构建资产概要文件。您也可以手动导入资产数据或编辑资产概要文件。有关更多信息，请参阅《*IBM QRadar User Guide*》中的主题导入资产概要文件和添加或编辑资产概要文件。

限制: 如果安装了 IBM QRadar Vulnerability Manager，那么 IBM QRadar Log Manager 仅跟踪资产数据。有关 QRadar SIEM 与 QRadar Log Manager 之间的差异的更多信息，请参阅 第 7 页的『IBM QRadar 产品中的功能』。

相关概念

IBM QRadar 产品中的功能

资产数据的源

资产数据接收自 IBM QRadar 部署中的若干不同的源。

资产数据会递增写入到资产数据库中（通常一次两个或三个数据段）。除网络漏洞扫描程序进行的更新以外，每个资产更新一次仅包含有关一个资产的信息。

资产数据通常来自以下资产数据源之一：

事件

事件有效内容（如 DHCP 或认证服务器创建的有效内容）通常包含用户登录、IP 地址、主机名、MAC 地址和其他资产信息。此数据会立即提供给资产数据库，以帮助确定资产更新适用于的资产。

事件是资产增长偏差的主要原因。

流数量

流有效内容包含按定期、可配置时间间隔收集的通信信息，如 IP 地址、端口和协议。在每个时间间隔结束时，会将数据提供给资产数据库（一次一个 IP 地址）。

由于流中的资产数据根据单一标识（即 IP 地址）与资产配对，因此流数据绝不会导致资产增长偏差。

漏洞扫描程序

QRadar 与 IBM 和第三方漏洞扫描程序集成，这些漏洞扫描程序可以提供资产数据，如操作系统、已安装的软件和补丁信息。数据的类型根据扫描程序而异，并且可以因扫描而异。随着新的资产、端口信息和漏洞的发现，会根据扫描中定义的 CIDR 范围将数据引入到资产概要文件中。

扫描程序可能会造成资产增长偏差，但是该情况比较少见。

用户界面

具有“资产”角色的用户可以将资产信息直接导入到或提供给资产数据库。由用户直接提供的资产更新用于特定资产。因此会绕过资产协调阶段。

用户提供的资产更新不会造成资产增长偏差。

域感知资产数据

使用域信息来配置资产数据源时，来自该数据源的所有资产数据都自动通过同一个域进行标记。由于资产模型中的数据可感知域，因此域信息会应用于所有 QRadar 组件，包括身份、攻击、资产概要文件和服务器发现。

查看资产概要文件时，某些字段可能为空白。当系统在资产更新中未接收此信息，或者信息超过资产保留期时，空白字段存在。缺省保留期为 120 天。显示为 0.0.0.0 的 IP 地址指示资产不包含 IP 地址信息。

传入的资产数据工作流程

IBM QRadar 在事件有效内容中使用身份信息来确定创建新资产还是更新现有资产。

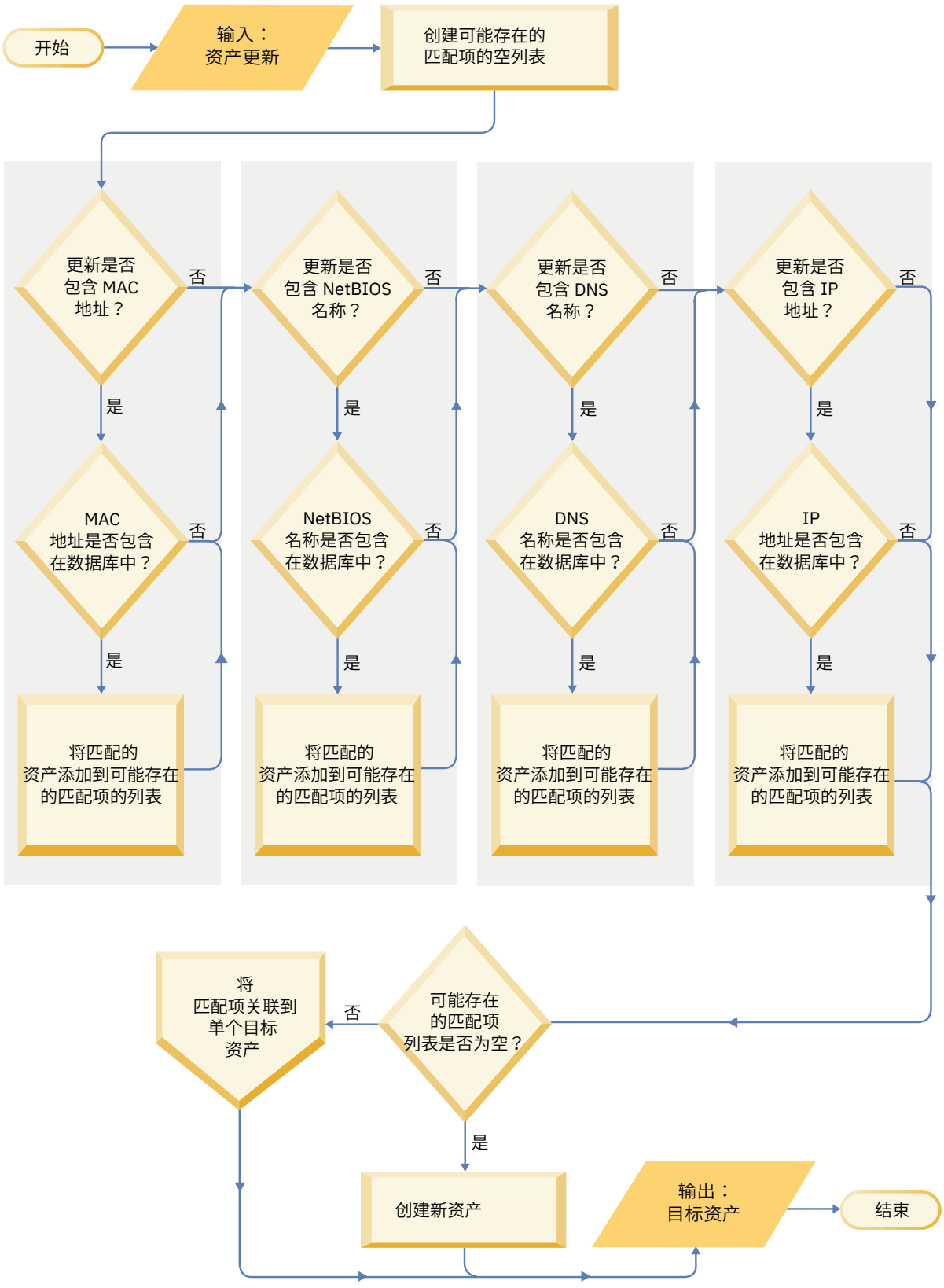

图 *18.* 资产数据工作流程图

1. QRadar 接收事件。资产概要分析程序将检查事件有效内容以获取身份信息。

2. 如果身份信息包含已与资产数据库中的资产关联的 MAC 地址、NetBIOS 主机名或 DNS 主机名，那么该资产将使用任何新信息进行更新。
3. 如果唯一的可用身份信息是 IP 地址，那么系统会协调对具有同一 IP 地址的现有资产的更新。
4. 如果资产更新具有与现有资产匹配的 IP 地址，但其他身份信息与现有资产不匹配，那么在更新现有资产之前，系统会使用其他信息来排除误报匹配。
5. 如果身份信息与数据库中的现有资产不匹配，那么将根据事件有效内容中的信息创建新资产。

资产数据更新

IBM QRadar 在事件有效内容中使用身份信息来确定要创建新资产还是更新现有资产。

每个资产更新都必须包含有关单个资产的可信信息。当 QRadar 接收资产更新时，系统会确定更新应用于的资产。

资产协调是确定资产更新与资产数据库中的相关资产之间关系的过程。资产协调在 QRadar 接收更新后但在信息写入到资产数据库中之前发生。

身份信息

每个资产都必须包含至少一段身份数据。包含一段或多段该相同身份数据的后续更新会与拥有该数据的资产进行协调。将会仔细处理基于 IP 地址的更新，以避免误报资产匹配。当一个物理资产分配有先前由系统中的另一个资产所有的 IP 地址的所有权时，会发生误报资产匹配。

当提供了多段身份数据时，资产概要分析程序按以下顺序从最为确定到最不确定划分信息优先级：

- MAC 地址
- NetBIOS 主机名
- DNS 主机名
- IP 地址

MAC 地址、NetBIOS 主机名和 DNS 主机名是唯一的，因此被视为最终身份数据。仅按 IP 地址与现有资产匹配的入局更新的处理方式不同于与更确定的身份数据匹配的更新。

资产协调排除规则

通过进入 IBM QRadar 的每个资产更新，资产协调排除规则将测试应用于资产更新中的 MAC 地址、NetBIOS 主机名、DNS 主机名和 IP 地址。

缺省情况下，会对每个资产数据段进行为期两小时的跟踪。如果资产更新中的任何一段身份数据在 2 小时内展现两次或以上的可疑行为，那么会将该数据段添加到资产黑名单。测试的每种类型的身份资产数据会生成新的黑名单。

在域感知环境中，资产协调排除规则为每个域单独跟踪资产数据的行为。

资产协调排除规则测试以下场景：

表 *31.* 规则测试和响应

场景	规则响应
MAC 地址在 2 小时或更短时间内与三个或更多不同 IP 地址关联	将 MAC 地址添加到资产协调域 MAC 黑名单
DNS 主机名在 2 小时或更短时间内与三个或更多不同 IP 地址关联	将 DNS 主机名添加到资产协调域 DNS 黑名单
NetBIOS 主机名在 2 小时或更短时间内与三个或更多不同 IP 地址关联	将 NetBIOS 主机名添加到资产协调域 NetBIOS 黑名单
IPv4 地址在 2 小时或更短时间内与三个或更多不同 MAC 地址关联	将 IP 地址添加到资产协调域 IPv4 黑名单

表 31. 规则测试和响应 (续)	
场景	**规则响应**
NetBIOS 主机名在 2 小时或更短时间内与三个或更多不同 MAC 地址关联	将 NetBIOS 主机名添加到资产协调域 NetBIOS 黑名单
DNS 主机名在 2 小时或更短时间内与三个或更多不同 MAC 地址关联	将 DNS 主机名添加到资产协调域 DNS 黑名单
IPv4 地址在 2 小时或更短时间内与三个或更多不同 DNS 主机名关联	将 IP 地址添加到资产协调域 IPv4 黑名单
NetBIOS 主机名在 2 小时或更短时间内与三个或更多不同 DNS 主机名关联	将 NetBIOS 主机名添加到资产协调域 NetBIOS 黑名单
MAC 地址在 2 小时或更短时间内与三个或更多不同 DNS 主机名关联	将 MAC 地址添加到资产协调域 MAC 黑名单
地址在 2 小时或更短时间内与三个或更多不同 NetBIOS 主机名关联	将 IP 地址添加到资产协调域 IPv4 黑名单
DNS 主机名在 2 小时或更短时间内与三个或更多不同 NetBIOS 主机名关联	将 DNS 主机名添加到资产协调域 DNS 黑名单
MAC 地址在 2 小时或更短时间内与三个或更多不同 NetBIOS 主机名关联	将 MAC 地址添加到资产协调域 MAC 黑名单

您可以在**攻击**选项卡上查看这些规则，方法是单击**规则**，然后在下拉列表中选择**资产协调排除**组。

资产合并

资产合并是一个资产的信息与另一个资产的信息进行组合的过程（前提是两个资产实际是同一物理资产）。

当资产更新包含与两个不同资产概要文件匹配的身份数据时，会发生资产合并。例如，如果单个更新包含与一个资产概要文件匹配的 NetBIOS 主机名和与另一个资产概要文件匹配的 MAC 地址，那么该更新可能会触发资产合并。

某些系统会导致大量资产合并，因为它们具有会在无意间将两个不同物理资产的身份信息组合成单个资产更新的资产数据源。这些系统的一些示例包括以下环境：

- 充当事件代理的中央系统日志服务器
- 虚拟机
- 自动化安装环境
- 非唯一主机名，与 iPad 和 iPhone 之类的资产通用。
- 具有共享 MAC 地址的虚拟专用网
- 日志源扩展，其中身份字段为 `OverrideAndAlwaysSend=true`

具有多个 IP 地址、MAC 地址或主机名的资产在资产增长中显示偏差，并且会触发系统通知。

识别资产增长偏差

有时，资产数据源会生成必须在进行手动补救后 IBM QRadar 才能正确处理的更新。根据异常资产增长的原因，您可以修正引起此问题的资产数据源，也可以阻止来自该数据源的资产更新。

当单个设备的资产更新数超过特定类型身份信息的保留时间阈值所设置的限制时，就会发生资产增长偏差。对于维护准确的资产模型而言，正确处理资产增长偏差至关重要。

导致每项资产增长偏差的根本原因是资产数据源，该数据源的数据不可信，不应用于更新资产模型。识别潜在的资产增长偏差之后，您必须检查信息源，以确定是否能够合理解释该资产为何积累大量身份数据。资产增长偏差的原因特定于环境。

资产概要文件中异常数据增长的 DHCP 服务器示例

假定动态主机配置协议 (DHCP) 网络中有一个虚拟专用网 (VPN) 服务器。该 VPN 服务器配置为通过代表客户机将 DHCP 请求以代理形式发送到该网络的 DHCP 服务器，从而将 IP 地址分配给入局 VPN 客户机。

从 DHCP 服务器的角度来说，同一 MAC 地址重复请求许多 IP 地址分配。在进行网络操作的情况下，VPN 服务器会将 IP 地址委派给客户机，但 DHCP 服务器无法在请求由一个资产代表另一个资产发出时进行区分。

DHCP 服务器日志（配置为 QRadar 日志源）会生成 DHCP 应答 (DHCP ACK) 事件，该事件将 VPN 服务器的 MAC 地址与它分配给 VPN 客户机的 IP 地址关联。发生资产协调时，系统会按 MAC 地址协调此事件，从而导致生成针对所解析的每个 DHCP ACK 事件按一个 IP 地址增长的单个现有资产。

最终，一个资产概要文件会包含分配给 VPN 服务器的每个 IP 地址。包含多个资产的相关信息的资产更新导致了此资产增长偏差。

阈值设置

当数据库中的资产达到特定的属性数量（例如，多个 IP 地址或 MAC 地址）时，QRadar 会阻止该资产接收更多更新。

资产概要分析程序阈值设置用于指定在何种条件下阻止资产更新。通常，资产更新次数的最大值为阈值。当系统收集足够的数据而超过阈值时，资产会显示资产增长偏差。这将阻止资产的未来更新，直到修正增长偏差为止。

指示资产增长偏差的系统通知

IBM QRadar 会生成系统通知来帮助您识别和管理环境中的资产增长偏差。

以下系统消息指示 QRadar 已识别潜在的资产增长偏差：

- `The system detected asset profiles that exceed the normal size threshold`
- `The asset blacklist rules have added new asset data to the asset blacklists`

系统通知消息包含一些链接，这些链接指向用于帮助您识别存在增长偏差的资产的报告。

频繁更改的资产数据

资产增长可能由大量合法更改的资产数据所致，例如下列情况下的更改：

- 一台移动设备频繁地从一间办公室移动到另一间办公室，并且每次登录时都分配有新的 IP 地址。
- 连接到 IP 地址租约较短的公用 Wi-Fi（例如，大学校园中的公用 Wi-Fi）的设备在一个学期内可能会收集到大量资产数据。

示例：日志源扩展的配置错误如何导致资产增长偏差

配置不正确的定制日志源扩展会导致资产增长偏差。

通过解析位于中央日志服务器上的事件有效内容中的用户名，可以配置定制日志源扩展来向 IBM QRadar 提供资产更新。 将日志源扩展配置为覆盖事件主机名属性，以便定制日志源生成的资产更新始终指定中央日志服务器的 DNS 主机名。

日志源会生成许多全都具有同一主机名的资产更新，而不是由 QRadar 接收具有用户已登录到的资产的主机名的更新。

在此情况下，资产增长偏差由一个包含许多 IP 地址和用户名的资产概要文件导致。

对超过正常大小阈值的资产概要文件进行故障诊断

当单个资产下的数据累计超过所配置的身份数据阈值限制时，IBM QRadar 会生成以下系统通知。

```
The system detected asset profiles that exceed the normal size threshold
```

说明

通知的有效内容显示一个列表，其中包含五个偏差最频繁的资产以及系统将每个资产标记为增长偏差的原因。 如以下示例中所示，有效内容还显示资产尝试增长超过资产大小阈值的次数。

```
Feb 13 20:13:23 127.0.0.1 [AssetProfilerLogTimer]
com.q1labs.assetprofile.updateresolution.UpdateResolutionManager:
[INFO] [NOT:0010006101][192.0.2.83/- -] [-/- -]
The top five most frequently deviating asset profiles between
Feb 13, 2015 8:10:23 PM AST and Feb 13, 2015 8:13:23 PM AST:
[ASSET ID:1003, REASON:Too Many IPs, COUNT:508],
[ASSET ID:1002, REASON:Too many DNS Names, COUNT:93],
[ASSET ID:1001, REASON:Too many MAC Addresses, COUNT:62]
```

当资产数据超过所配置的阈值时，QRadar 会阻止资产将来进行更新。 此干预防止系统接收更多损坏的数据，并且降低在系统尝试针对异常大的资产概要文件来协调入局更新时可能出现的性能影响。

必需用户操作

使用通知有效内容中的信息来识别造成资产增长偏差的资产并确定导致异常增长的原因。 通知提供指向在过去 24 小时遭遇资产增长偏差的所有资产的报告的链接。

解决环境中的资产增长偏差后，可以再次运行报告。

1. 单击**日志活动**选项卡，然后单击**搜索 > 新建搜索**。
2. 选择保存的搜索**偏差资产增长：资产报告**。
3. 使用报告识别并修复在偏差期间创建的不准确资产数据。

相关概念

旧资产数据

在创建新资产记录的速率超过除去旧资产数据的速率时，旧资产数据可能发生问题。控制和管理资产保留时间阈值是解决旧资产数据导致的资产增长偏差的关键。

向资产黑名单中添加了新资产数据

当某个资产数据段所表现出的行为与资产增长偏差一致时，IBM QRadar 会生成以下系统通知。

```
The asset blacklist rules have added new asset data to the asset blacklists
```

说明

资产排除规则监视资产数据的一致性和完整性。 规则长期跟踪特定资产数据段，以确保在合理时间内通过与同一数据子集一致的方式对其进行观察。

例如，如果资产更新包含 MAC 地址和 DNS 主机名，那么 MAC 地址在某个持续时间段与该 DNS 主机名关联。 当资产更新中包含 DNS 主机名时，包含该 MAC 地址的后续资产更新也包含同一 DNS 主机名。 如果 MAC 地址突然短期与其他 DNS 主机名关联，那么会监视更改。 如果 MAC 地址短期内再次更改，那么会将 MAC 地址标记为可造成资产增长偏差或异常情况。

必需用户操作

使用通知有效内容中的信息来识别用于监视资产数据的规则。 单击通知中的**资产偏差（按日志源划分）**链接可查看过去 24 小时发生的资产偏差。

如果资产数据有效，那么 QRadar 管理员可以配置 QRadar 来解决问题。

- 如果黑名单的填充过于激烈，那么可以调整用于填充这些黑名单的资产协调排除规则。
- 如果要将数据添加到资产数据库中，那么可以从黑名单中除去资产数据并将其添加到对应的资产白名单。将资产数据添加到白名单可防止其在黑名单上意外重新出现。

相关概念

资产协调排除规则的高级调整

您可以调整资产协调排除规则来优化一个或多个规则中的资产增长偏差的定义。

资产增长偏差预防

在确认报告的资产增长合法后，可通过多种方式阻止 IBM QRadar 触发此资产的增长偏差消息。

使用以下列表以帮助您决定如何阻止资产增长偏差：

- 了解 QRadar 如何处理旧资产数据。
- 创建身份排除搜索以从提供资产更新中排除特定事件。
- 调整“资产协调排除”规则以优化偏差资产增长的定义。
- 创建资产白名单以阻止数据在资产黑名单上再次出现。
- 修改资产黑名单和白名单上的条目。
- 确保 DSM 为最新。QRadar 提供可能包含 DSM 更新和解析问题纠正的每周自动更新。

旧资产数据

在创建新资产记录的速率超过除去旧资产数据的速率时，旧资产数据可能发生问题。控制和管理资产保留时间阈值是解决旧资产数据导致的资产增长偏差的关键。

旧资产数据是在特定时间内未被主动或被动观测到的历史资产数据。旧资产数据超过配置的保留期时将删除。

如果 IBM QRadar 通过事件和流被动或者通过端口和漏洞扫描程序主动观测到历史记录，那么历史记录将再次变为活动。

避免资产增长偏差需要在针对单个资产分配的 IP 地址数量与 QRadar 保留数据的时间长度之间找到正确的平衡。在配置 QRadar 以适用高级别资产数据保留之前，必须考虑性能和可管理性折衷。虽然较长的保留期和较高的每个资产阈值可能始终是理想状态，但是更适合的方法是确定环境可接受的基线配置并测试此配置。然后，您可以小幅增加保留时间阈值直至实现适当的平衡。

资产黑名单和白名单

IBM QRadar 使用一组资产协调规则来确定资产数据是否可信。资产数据存疑时，QRadar 使用资产黑名单和白名单来确定是否使用资产数据来更新资产概要文件。

资产黑名单是 QRadar 认为不可信的数据集合。资产黑名单中的数据可能会导致出现资产增长偏差，因此 QRadar 会阻止将此数据添加到资产数据库中。

资产白名单是资产数据的集合，它覆盖有关要将哪些数据添加至资产黑名单的资产协调引擎逻辑。当系统识别黑名单匹配项时，它将检查白名单，以确定该值是否存在。如果该资产更新与白名单中的数据匹配，那么将协调该更改并更新该资产。列入白名单的资产数据针对所有域进行全局应用。

资产黑名单和白名单为参考集。您可使用 QRadar Console 中的“**参考集管理**”工具来查看和修改资产黑名单和白名单数据。有关处理参考集的更多信息，请参阅第 74 页的『参考集概述』。

资产黑名单

资产黑名单是一个数据集合，其中包含的数据是 IBM QRadar 根据资产协调排除规则确定的不可信数据。资产黑名单中的数据可能会导致出现资产增长偏差，因此 QRadar 会阻止将此数据添加到资产数据库中。

QRadar 中的每个资产更新都会与资产黑名单进行比较。将对所有域全局应用列入黑名单的资产数据。如果资产更新包含黑名单中找到的身份信息（MAC 地址、NetBIOS 主机名、DNS 主机名或 IP 地址），那么系统会废弃入局更新并且不会更新资产数据库。

下表显示了每种身份资产数据的引用集合名称和类型。

表 32. 资产黑名单数据的引用集合名称

身份数据的类型	引用集合名称	引用集合类型
IP 地址 (v4)	资产协调 IPv4 黑名单	引用集 [集类型：IP]
DNS 主机名	资产协调 DNS 黑名单	引用集 [集类型：ALNIC*]

表 32. 资产黑名单数据的引用集合名称 (续)		
身份数据的类型	**引用集合名称**	**引用集合类型**
NetBIOS 主机名	资产协调 NetBIOS 黑名单	引用集 [集类型：ALNIC*]
MAC 地址	资产协调 MAC 黑名单	引用集 [集类型：ALNIC*]
* ALNIC 是可以同时适应主机名值和 MAC 地址值的字母数字类型。		

您可以使用“**引用集管理**”工具来编辑黑名单条目。有关使用引用集的信息，请参阅引用集管理 (http://www.ibm.com/support/knowledgecenter/SS42VS_7.2.7/com.ibm.qradar.doc/c_qradar_adm_mge_ref_set.html)。

相关概念
资产白名单

资产白名单
您可使用资产白名单来确保 IBM QRadar 资产数据不会意外地重新出现在资产黑名单中。

资产白名单是资产数据的集合，它覆盖有关要将哪些数据添加至资产黑名单的资产协调引擎逻辑。当系统识别黑名单匹配项时，它将检查白名单，以确定该值是否存在。如果该资产更新与白名单中的数据匹配，那么将协调该更改并更新该资产。列入白名单的资产数据针对所有域进行全局应用。

您可以使用“**参考集管理**”工具来编辑白名单条目。有关使用参考集的信息，请参阅参考集管理。

白名单用例示例

存在继续出现在黑名单中的资产数据，而它是有效的资产更新时，白名单非常有用。例如，您可能有一个循环法 DNS 负载均衡器，它配置为循环使用 5 个 IP 地址。资产协调排除规则可能确定多个 IP 地址与同一个 DNS 主机名称相关联表明存在资产增长偏差，系统可将此 DNS 负载均衡器添加至黑名单。为了解决此问题，您可将这个 DNS 主机名添加至资产协调 DNS 白名单。

添加到资产白名单的大量条目

通过准确的资产数据库，可以更轻松地将系统中触发的攻击与网络中的物理资产和虚拟资产相关联。通过将大量条目添加到资产白名单来忽略资产偏差对于构建准确的资产数据库而言并无帮助。请勿添加大量的白名单条目，而应复查资产白名单，以确定导致资产增长偏差的因素，然后确定如何加以修正。

资产白名单的类型

每种类型的身份数据保留在单独的白名单中。下表显示了每种身份资产数据的参考集合名称和类型。

表 33. 资产白名单数据的参考集合名称		
数据类型	**参考集合名称**	**参考集合类型**
IP 地址	资产协调 IPv4 白名单	参考集 [集类型：IP]
DNS 主机名	资产协调 DNS 白名单	参考集 [集类型：ALNIC*]
NetBIOS 主机名	资产协调 NetBIOS 白名单	参考集 [集类型：ALNIC*]
MAC 地址	资产协调 MAC 白名单	参考集 [集类型：ALNIC*]

* ALNIC 是可以适应主机名值和 MAC 地址值的字母数字类型。

相关概念
资产黑名单

资产黑名单是一个数据集合，其中包含的数据是 IBM QRadar 根据资产协调排除规则确定的不可信数据。资产黑名单中的数据可能会导致出现资产增长偏差，因此 QRadar 会阻止将此数据添加到资产数据库中。

使用参考集实用程序更新资产黑名单和白名单

您可以使用 IBM QRadar 参考集实用程序来添加或修改位列资产黑名单或白名单上的条目。

要管理参考集，请从 QRadar Console 上的 /opt/qradar/bin 运行 ReferenceDataUtil.sh 实用程序。

下表中描述了用于将新值添加到各列表中的命令。参数值必须与始发资产数据源提供的资产更新值完全匹配。

表 *34.* 用于修改资产黑名单和白名单数据的命令语法

名称	命令语法

资产协调 IPv4 黑名单	`ReferenceDataUtil.sh add "Asset Reconciliation IPv4 Blacklist" IP`
	例如，此命令将 IP 地址 192.168.3.56 添加到黑名单：
	`ReferenceDataUtil.sh add "Asset Reconciliation IPv4 Blacklist" 192.168.3.56`

资产协调 DNS 黑名单	`ReferenceDataUtil.sh add "Asset Reconciliation DNS Blacklist" DNS`
	例如，此命令将域名“misbehaving.asset.company.com”添加到黑名单：
	`ReferenceDataUtil.sh add "Asset Reconciliation DNS Blacklist" "misbehaving.asset.company.com"`

资产协调 NetBIOS 黑名单	`ReferenceDataUtil.sh add "Asset Reconciliation NetBIOS Blacklist" NETBIOS`
	例如，此命令从黑名单中移除 NetBIOS 主机名“deviantGrowthAsset-156384”：
	`ReferenceDataUtil.sh delete "Asset Reconciliation NetBIOS Blacklist" "deviantGrowthAsset-156384"`

资产协调 MAC 黑名单	`ReferenceDataUtil.sh add "Asset Reconciliation MAC Blacklist" MACADDR`
	例如，此命令将 MAC 地址“00:a0:1a:2b:3c:4d”添加到黑名单：
	`ReferenceDataUtil.sh add "Asset Reconciliation MAC Blacklist" "00:a0:1a:2b:3c:4d"`

资产协调 IPv4 白名单	`ReferenceDataUtil.sh add "Asset Reconciliation IPv4 Whitelist" IP`
	例如，此命令从白名单中删除 IP 地址 10.1.95.142：
	`ReferenceDataUtil.sh delete "Asset Reconciliation IPv4 Whitelist" 10.1.95.142`

资产协调 DNS 白名单	`ReferenceDataUtil.sh add "Asset Reconciliation DNS Whitelist" DNS`
	例如，此命令将域名“loadbalancer.company.com”添加到白名单：
	`ReferenceDataUtil.sh add "Asset Reconciliation DNS Whitelist" "loadbalancer.company.com"`

资产协调 NetBIOS 白名单	`ReferenceDataUtil.sh add "Asset Reconciliation NetBIOS Whitelist" NETBIOS`
	例如，此命令将 NetBIOS 名称“assetName-156384” 添加到白名单：
	`ReferenceDataUtil.sh add "Asset Reconciliation NetBIOS Whitelist" "assetName-156384"`

表 *34.* 用于修改资产黑名单和白名单数据的命令语法 *(续)*	
名称	**命令语法**

资产协调 MAC 白名单	`ReferenceDataUtil.sh add "Asset Reconciliation MAC Whitelist" MACADDR`
	例如，此命令将 MAC 地址“00:a0:1a:2b:3c:4d”添加到白名单：
	`ReferenceDataUtil.sh add "Asset Reconciliation MAC Whitelist" "00:a0:1a:2b:3c:4d"`

相关任务

使用 RESTful API 来更新黑名单和白名单

使用 RESTful API 来更新黑名单和白名单

您可使用 IBM QRadar RESTful API 来定制资产黑名单和白名单的内容。

关于此任务

您必须指定所要查看或更新的参考集的确切名称。

· 资产协调 IPv4 黑名单
· 资产协调 DNS 黑名单
· 资产协调 NetBIOS 黑名单
· 资产协调 MAC 黑名单
· 资产协调 IPv4 白名单
· 资产协调 DNS 白名单
· 资产协调 NetBIOS 白名单
· 资产协调 MAC 白名单

过程

1. 在 Web 浏览器中输入下列 URL，以访问 RESTful API 界面：

   ```
   https://ConsoleIPaddress/api_doc
   ```

2. 在左侧的导航窗格中，查找 `4.0>/reference_data >/sets > /{name}`。
3. 要查看资产黑名单或白名单的内容，请完成下列步骤：
   a) 单击 **GET** 选项卡，向下滚动到**参数**部分。
   b) 在**名称**参数的**值**字段中，输入您想要查看的资产黑名单或白名单的名称。
   c) 单击**尝试**，然后在屏幕底部查看结果。
4. 要将某个值添加到资产黑名单或白名单，请完成下列步骤：
   a) 单击 **POST** 选项卡，向下滚动到**参数**部分。
   b) 输入下列参数的值：

表 *35.* 添加新资产数据所需的参数	
参数名称	**参数描述**
name	表示要更新的参考集的名称。
value	表示要添加到资产黑名单或白名单的数据项。必须与起始资产数据源所提供的资产更新值完全匹配。

   c) 单击**尝试**，以将新值添加到资产白名单或资产黑名单。

下一步做什么

有关使用 RESTful API 来更改参考集的更多信息，请参阅 *IBM QRadar API Guide*。

相关概念

使用参考集实用程序更新资产黑名单和白名单

您可以使用 IBM QRadar 参考集实用程序来添加或修改位列资产黑名单或白名单上的条目。

身份排除搜索

身份排除搜索可用于管理出于已知的正当理由而累积大量类似身份信息的单个资产。

例如，日志源可以向资产数据库提供大量资产身份信息。它们为 IBM QRadar 提供近乎实时的资产信息更改，并且可以保持资产数据库为最新内容。但是，日志源在大多数情况下是资产增长偏差以及其他与资产相关的异常的来源。

当日志源将错误的资产数据发送到 QRadar 时，请尝试修正日志源，以便其发送的数据可供资产数据库使用。如果无法修正日志源，那么可以构建身份排除搜索，用于阻止资产信息进入资产数据库。

您还可以使用身份排除搜索（其中 `Identity_Username+Is Any Of + Anonymous Logon`）来确保未在更新与服务帐户或自动化服务相关的资产。

身份排除搜索和黑名单之间的差异

虽然身份排除搜索貌似与资产黑名单功能类似，但是存在显著差异。

黑名单只能指定要排除的原始资产数据，例如 MAC 地址和主机名。身份排除搜索根据日志源、类别和事件名称之类的搜索字段来过滤输出资产数据。

黑名单不会将提供数据的数据源的类型列入在内，而身份排除搜索只能应用于事件。 身份排除搜索可以根据常用事件搜索字段（例如事件类型、事件名称、类别和日志源）来阻止资产更新。

资产协调排除规则的高级调整

您可以调整资产协调排除规则来优化一个或多个规则中的资产增长偏差的定义。

例如，请考虑资产协调排除规则中的此规范化模板。

```
Apply AssetExclusion: Exclude DNS Name By IP on events which are detected
 by the Local system and NOT when any of
Identity Host Name are contained in any of
Asset Reconciliation DNS Whitelist - AlphaNumeric (Ignore Case),
 Asset Reconciliation DNS Blacklist - AlphaNumeric (Ignore Case)
 and when at least N1 events are seen with the same
Identity Host Name and different Identity IP in N2
```

此表列出规则模板中可以调整的变量以及更改的结果。请避免更改模板中的其他变量。

表 *36*. 用于调整资产协调规则的选项

变量	缺省值	调整结果
N1	3	将此变量调整为更低的值会导致更多数据添加到黑名单，因为需要更少的具有冲突数据的事件以使规则触发。 将此变量调整为更高的值会导致更少数据添加到黑名单，因为需要更多具有冲突数据的事件以使规则触发。
N2	2 小时	将此变量调整为更低的值会减小必须看到 N1 事件以使规则触发的时间窗口。观察匹配数据所需的时间会减少，从而导致更少数据添加到黑名单。 将此变量调整为更高的值会增大必须看到 N1 事件以使规则触发的时间窗口。观察匹配数据所需的时间会增加，从而导致更多数据添加到黑名单。 增大时间段可能会影响系统内存资源，因为会在更长的时间段内对数据进行跟踪。

资产协调排除规则是系统范围规则。 对规则的更改会影响规则在整个系统中的行为方式。

对规则应用不同调整

可能有必要在系统的不同部分中对规则应用不同调整。要对规则应用不同调整，必须复制要调整的资产协调排除规则并添加一个或多个测试来约束规则，以便仅测试系统的某些部分。例如，可能要创建仅测试网络、日志源或事件类型的规则。

关于此任务

向系统添加新规则时请始终谨慎，因为一些任务和 CRE 规则可能会影响系统性能。 以下做法可能有益：将新规则添加到每个测试堆栈的顶部，从而只要资产更新与新规则的条件匹配，便允许系统绕过测试逻辑的其余部分。

过程

1. 复制规则。
   a) 在**攻击**选项卡上，单击**规则**并选择要复制的规则。
   b) 单击**操作 > 复制**。
      如果新规则的名称指示复制该规则的原因，那么可能会有所帮助。
2. 向规则添加测试。

   确定要用于将规则仅应用到系统数据子集的过滤器。例如，可以添加仅与来自特定日志源的事件匹配的测试。
3. 调整规则的变量以实现所需行为。
4. 更新原始规则。
   a) 将已添加到重复规则的同一测试添加到原始规则，但是这次反转规则 AND 和 AND NOT 运算符。

      反转运算符会防止在两个规则中均触发事件。

示例：调整为从黑名单中排除 IP 地址的资产排除规则

您可以通过调整资产排除规则使 IP 地址避免列入黑名单。

作为网络安全性管理员，您管理的是包含公共 wifi 网段的公司网络，其中 IP 地址租赁通常时间短且频繁。此网段上的资产趋于瞬态，主要是频繁登录和注销公共 wifi 的笔记本和手持设备。 通常，一个 IP 地址在短期内由不同设备多次使用。

在其余部署中，您具有一个仔细管理的网络，其中仅包含已盘点的知名公司设备。 IP 地址在此部分的网络中租赁时间更长，并且 IP 地址仅通过认证进行访问。 在此网段上，您希望在有任何资产增长偏差时立即获知情况，并且保留资产协调排除规则的缺省设置。

将 IP 地址列入黑名单

在此环境中，缺省资产协调排除规则会无意间将整个网络短期列入黑名单。

您的安全团队发现 wifi 网段生成的资产相关通知惹人讨厌。 您希望防止 wifi 触发任何其他偏差资产增长通知。

调整资产协调规则以忽略某些资产更新

复审上次系统通知中的**由日志源导致的资产偏差**报告。 确定列入黑名单的数据是来自 您的 wifi 上的 DHCP 服务器。

与**资产排除：按 MAC 地址排除 IP** 规则对应的行的**事件计数**列、**流计数**列和**攻击**列中的值指示是您的 wifi DHCP 服务器在触发此规则。

向现有资产协调排除规则中添加测试可阻止规则将 wifi 数据添加到黑名单。

```
Apply AssetExclusion:Exclude IP by MAC address on events which are detected by
the Local system and NOT when the event(s) were detected by one or more of
MicrosoftDHCP @ microsoft.dhcp.test.com
and NOT when any of Domain is the key and any of Identity IP is the value in
any of Asset Reconciliation Domain IPv4 Whitelist
- IP Asset Reconciliation Domain IPv4 Blacklist - IP
```

```
and when at least 3 events are seen with the same Identity IP and
different Identity MAC in 2 hours.
```

已更新的规则仅测试来自您的 wifi DHCP 服务器上没有的日志源的事件。 为防止 Wi-Fi DHCP 事件经历成本更高的引用集和行为分析测试，您还将此测试移至测试堆栈的顶部。

出现增长偏差后清理资产数据

IBM QRadar 使用资产模型将部署中的攻击连接到网络中的物理或虚拟资产。收集和查看有关资产使用方式的相关数据的能力是解决安全性问题中的重要步骤。维护资产数据库以确保数据保持更新和准确性至关重要。

无论是解决问题根源还是阻止资产更新，都必须通过移除无效资产数据和移除资产黑名单条目来清理资产数据库。

删除黑名单条目

修正黑名单条目的原因之后，必须清除残留的条目。您可移除个别的黑名单条目，但最好清除所有的黑名单条目，并允许与资产增长偏差无法的黑名单值重新生成。

过程

要使用 IBM QRadar 控制台来清除黑名单，请执行下列操作：

a) 在导航菜单（☰）上，单击**管理**。

b) 在**系统配置**部分中，单击**参考集管理**。

c) 选择参考集，然后单击**删除**。

d) 使用快速搜索文本框来搜索您想要删除的参考集，然后单击**删除所列项**。

结果

清除黑名单会移除全部黑名单条目，包括手动添加的条目。手动添加的黑名单条目必须重新添加。

第 16 章 事件存储转发

使用“存储转发”功能来管理调度以将事件从专用 事件收集器 设备转发到部署中的事件处理器组件。

在 Event Collector 1501 和 Event Collector 1590 上支持“存储转发”功能。有关这些设备的更多信息，请参阅 *IBM QRadar* 硬件指南。

专用 事件收集器 不处理事件并且不包含板载事件处理器。缺省情况下，专用事件收集器持续将事件转发到连接到 QRadar 的事件处理器。

您可以调度想要事件收集器将事件转发到事件处理器的时间范围。通过在非工作时间转发事件，可以确保传输不会对网络带宽造成负面影响。在调度事件转发时，事件将本地存储在事件收集器上，直至转发调度启动。在此时间内，无法在 IBM QRadar 控制台中查看事件。

相关概念

IBM QRadar 产品中的功能

第 17 章 安全性内容

您可使用 IBM QRadar 中的内容管理工具来将安全性内容（例如，规则、报告、仪表板和应用程序）导入 QRadar。安全性内容可来自任何其他 QRadar 系统，或者可独立开发安全性内容以扩展现有 QRadar 功能。

相关概念

IBM QRadar 产品中的功能

安全性内容的类型

IBM QRadar 内容捆绑到两种类型：内容包和扩展。

内容包

安全性内容包包含对特定类型的安全内容的增强功能。通常其中包含适用于第三方集成或操作系统的内容。例如，适用于第三方集成的安全性内容包可能包含新的定制事件属性，以便使事件有效内容中的信息可供日志源搜索且可用于报告。

安全性内容包可从 IBM Fix Central (http://www.ibm.com/support/fixcentral) 获取。内容包不作为自动更新的一部分提供。

扩展

IBM 和其他供应商会编写安全性扩展以增强或扩展 QRadar 功能。扩展可包含应用程序、内容项（例如，定制规则、报告模板、已保存的搜索）或者包含对现有内容项的更新。例如，扩展可包含一个应用程序，用于在 QRadar 添加一个选项卡以便为攻击提供可视化。

在 IBM Security App Exchange 上，扩展被称为应用程序。您可从 IBM Security App Exchange 下载 QRadar 应用程序，并使用**扩展管理**工具来进行安装。应用程序不作为自动更新的一部分提供。

安全性内容的来源

QRadar 内容可从以下来源获取：

IBM Security App Exchange

IBM Security App Exchange (https://apps.xforce.ibmcloud.com) 是一个应用程序库和门户网站，您可在其中浏览并下载 QRadar 扩展。它是一种共享、代码、可视化、报告、规则和应用程序的新方法。

IBM Fix Central

IBM Fix Central (www.ibm.com/support/fixcentral) 可为系统软件、硬件和操作系统提供修订和更新。您可从 IBM Fix Central 下载安全性内容包和扩展。

QRadar 部署

您可从 QRadar 部署导出定制内容以作为扩展，然后要复用内容时将其导入其他系统。例如，您将内容从开发环境导出至生产环境。您可使用内容管理脚本来导出所有内容，或者也可以选择仅导出部分定制内容。

导入和导出内容的方法

您可使用以下工具在自己的 IBM QRadar 部署中导入和导出内容。

扩展管理工具

使用“**扩展管理**”工具来为 QRadar 部署添加扩展。使用“**扩展管理**”工具导入内容时，可在安装前查看其内容。如果内容项已存在于系统中，那么可以指定替换内容项还是跳过更新。

无法使用“**扩展管理**”工具来导出内容。

DSM 编辑器

在 QRadar V7.3.3 和更高版本中，您可以导出在 DSM 编辑器中创建的定制内容。单击 DSM 编辑器中的**导出**按钮，将您的内容从一个 QRadar 部署导出到另一个部署，或导出到外部介质。

注: 可以从更低版本的 QRadar 导出内容并将其导入到更高版本中。但是，不能将内容从更高版本导入到更低版本中。

注: 如果将覆盖规则从一个 QRadar 部署移至另一个部署，请使用**替换现有内容项**选项来确保正确导入这些规则。

使用扩展管理安装扩展

使用**扩展管理**工具将安全扩展添加到 IBM QRadar。通过**扩展管理**工具，可以在安装扩展之前查看扩展中的内容项并指定处理内容更新的方法。

开始之前

在 QRadar 中安装扩展之前，这些扩展必须位于本地计算机上。

可以从 IBM Security App Exchange (https://apps.xforce.ibmcloud.com/) 和 IBM Fix Central (www.ibm.com/support/fixcentral/) 下载 QRadar 扩展。

关于此任务

扩展是 QRadar 功能束。扩展可以包含诸如规则、报告、搜索、参考集和仪表板之类的内容。它还可包含用于增强 QRadar 功能的应用程序。

过程

1. 在导航菜单（☰）上，单击**管理**。
2. 在**系统配置**部分中，单击**扩展管理**。
3. 要将新扩展上载到 QRadar 控制台，请完成下列步骤:
   a) 单击**添加**。
   b) 单击**浏览**并浏览查找扩展。
   c) 单击**立即安装**以安装扩展而不查看内容。转至 第 134 页的『5.b』。
   d) 单击**添加**。
4. 要查看扩展的内容，请从扩展列表中选择扩展，然后单击**更多详细信息**。
5. 要安装扩展，请完成下列步骤:
   a) 从列表中选择扩展，然后单击**安装**。
   b) 要向应用程序分配用户，请选择**用户选择**菜单，然后选择用户。
   例如，您可能希望将应用程序与**用户选择**菜单中具有已定义的许可权的指定用户相关联。

   注:

   仅当扩展中的您正在安装的任何应用程序配置为请求后台进程认证时，才会显示此屏幕。
   c) 如果扩展不包含数字签名，或者它已签署但签名未与 IBM 安全认证中心 (CA) 关联，那么您必须确认是否仍要对其进行安装。单击**安装**以继续安装。
   d) 复审安装对系统进行的更改。
   e) 选择**保留现有项**或**替换现有项**以指定如何处理现有内容项。

   注: 如果扩展包含已覆盖的系统规则，请选择**替换现有项**以确保正确导入规则。
   f) 单击**安装**。
   g) 复审安装摘要并单击**确定**。

卸载内容扩展

移除不再有用或对于您的系统有负面影响的内容扩展。您可移除规则、定制属性、参考数据和保存的搜索。您可能无法移除部分内容（如果有其他内容项依赖于该内容）。

关于此任务

卸载内容扩展时，任何由该内容扩展安装的规则、定制属性和参考数据都会移除，或还原为其先前状态。已保存的搜索不可还原。它们只能移除。

例如，如果您已使用现在想要卸载的应用程序来编辑定制规则，您可保留每个定制规则的更改。如果该定制规则先前存在于系统上，您可将该规则还原为之前的状态。如果该定制规则先前不存在，您可移除它。

注:

如果您已引入对该应用程序所安装内容扩展的外部依赖关系，那么您卸载应用程序时，QRadar 不会移除该内容。例如，如果您所创建的定制规则使用该应用程序的某个定制属性，那么您卸载应用程序时，不会移除该定制属性。

过程

1. 在导航菜单（☰）上，单击**管理**。
2. 在**系统配置**部分中，单击**扩展管理**。
3. 选择您想要卸载的扩展，然后单击**卸载**。

   QRadar 检查该内容扩展所安装的应用程序、规则、定制属性、参考数据及已保存的搜索，确定是否有任何可移除的项。
4. 如果在安装该应用程序之后，您已手动更改任何规则、定制属性或参考数据，请选择是要**保留**还是**移除/还原**该内容扩展。
5. 单击**卸载**，然后单击**确定**。

用于导出定制内容的内容类型标识

从 IBM QRadar 导出特定类型的定制内容时，必须指定内容类型。必须针对此内容类型使用文本标识或数字标识。

从 QRadar 设备导出内容时，内容管理脚本会检查内容依赖关系，然后在导出中包含关联的内容。

例如，当内容管理脚本检测到已保存的搜索与要导出的报告关联时，会同时导出已保存的搜索。无法导出已保存的攻击搜索、资产搜索或漏洞搜索。

要导出特定类型的所有定制内容时，可使用内容类型标识。如果要从 QRadar 部署导出特定内容项，必须知道此特定内容项的唯一标识。

下表描述了传递到 **-c** 参数的 `contentManagement.pl` 脚本的内容类型标识。

表 *37.* 用于导出定制内容的内容类型标识

定制内容类型	**文本标识**	**数字标识**
所有定制内容	**all**	不适用
定制内容列表	**package**	不适用
仪表板	**仪表板**	4
报告	**报告 (report)**	10
已保存的搜索	**搜索**	1
FGroups [1]	**fgroup**	12
FGroup 类型	**fgrouptype**	13

表 37. 用于导出定制内容的内容类型标识 (续)

定制内容类型	文本标识	数字标识
定制规则	**customrule**	3
定制属性	**customproperty**	6
日志源	**sensordevice**	17
日志源类型	**sensordevicetype**	24
日志源类别	**sensordevicecategory**	18
日志源扩展	**deviceextension**	16
参考数据集合	**referencedata**	28
定制 QID 映射条目	**qidmap**	27
历史相关性概要文件	**historicalsearch**	25
定制函数	**custom_function**	77
定制操作	**custom_action**	78
应用程序	**installed_application**	100

[1]FGroup 是内容组，如日志源组、报告组或搜索组。

第 18 章 SNMP 陷阱配置

IBM QRadar 使用 Net-SNMP 代理程序，这支持各种系统资源监视 MIB。网络管理解决方案可轮询它们以用于系统资源监视和警报。有关 Net-SNMP 的更多信息，请参阅 Net-SNMP 文档。

在 IBM QRadar 中，您可以配置规则以生成在满足配置的条件时发送 SNMP 陷阱的规则响应。QRadar 充当代理程序以将 SNMP 陷阱发送到另一个系统。

简单网络管理协议 (SNMP) 陷阱是 QRadar 发送到配置的 SNMP 主机以进行额外处理的事件或攻击通知。

在定制规则向导中定制 SNMP 配置参数并修改定制规则引擎发送到其他软件以用于管理的 SNMP 陷阱。QRadar 提供两个缺省陷阱。但是，您可以添加定制陷阱或修改现有陷阱以使用新参数。

有关 SNMP 的更多信息，请转至 The Internet Engineering Task Force (http://www.ietf.org/) Web 站点并在搜索字段中输入 RFC 1157。

相关概念

IBM QRadar 产品中的功能

第 19 章 敏感数据保护

配置数据模糊处理概要文件以避免未经授权访问 IBM QRadar 中的敏感或个人可标识信息。

数据模糊处理是从战略上向 QRadar 用户隐藏数据的过程。您可以隐藏定制属性、规范化属性（例如，用户名），或者您可以隐藏有效内容的内容（例如，信用卡或社保编号）。

针对有效内容和规范化消息，对数据模糊处理概要文件中的表达式求值。如果数据匹配模糊处理表达式，那么将在 QRadar 中隐藏数据。数据可以向所有用户隐藏，或者仅向属于特定域或租户的用户隐藏。尝试直接查询数据库的受影响的用户无法看到敏感数据。必须通过上载创建数据模糊处理概要文件时生成的专用密钥将数据转换为原始格式。

为确保 QRadar 仍可关联隐藏的数据值，加密过程是确定的。每次找到数据时，都显示相同的字符集。

相关概念

IBM QRadar 产品中的功能

数据模糊处理的工作原理

在 IBM QRadar 部署中配置数据模糊处理前，必须了解它是如何配合全新和现有的攻击、资产和日志源扩展运行的。

现有事件数据

启用数据模糊处理概要文件时，系统会为每个事件屏蔽 QRadar 接收到的数据。配置数据模糊处理前设备接收到的事件会保持处于原先未经模糊处理的状态。不屏蔽较旧的信息，用户可查看这些信息。

资产

配置数据模糊处理时，资产模型会累积屏蔽的数据，而原先已存在的资产模型数据会保持处于不屏蔽状态。

要防止有人使用未屏蔽的数据来跟踪已经过模糊处理的信息，请清除资产模型数据以除去未经屏蔽的数据。QRadar 将使用经过模糊处理的值来重新填充资产数据库。

攻击

未确保攻击不显示先前未屏蔽的数据，请重置 SIM 模型以关闭所有现有攻击。有关更多信息，请参阅第 31 页的『重置 SIM』。

规则

您必须更新依赖于先前未屏蔽的数据的规则。例如，对用户名进行模糊处理时，不会触发依赖于特定用户名的规则。

日志源扩展

更改事件有效内容格式的日志源扩展可能导致数据模糊处理出现问题。

数据模糊处理概要文件

包含要屏蔽的数据的相关信息的数据模糊处理概要文件。它还会跟踪解密数据所需的密钥库。

已启用的概要文件

仅当确定表达式对应的要进行模糊处理的数据目标正确时，才启用概要文件。如果要在启用数据模糊处理概要文件前测试正则表达式，可以创建基于正则表达式的定制属性。

启用的概要文件会立即开始按概要文件中启用的表达式定义的方式对数据进行模糊处理。已启用的概要文件会被自动锁定。仅限具有专用密钥的用户才能在启用概要文件后对其进行禁用或更改。

为确保经过模糊处理的数据可回溯至模糊处理概要文件，不得删除已启用的概要文件，即使将其禁用后也是如此。

已锁定的概要文件

启用概要文件会，会将其自动锁定，或者您可手动将其锁定。

锁定的概要文件具有以下限制：

- 您无法对其进行编辑。
- 您无法将其启用或禁用。您必须提供密钥库并将概要文件解锁后才能对其进行更改。
- 您无法将其删除，即使将其解锁后也是如此。
- 如果对已锁定的概要文件使用密钥库，那么将自动锁定使用该密钥库的所有其他概要文件。

下表显示了已锁定或已解锁的概要文件示例：

表 *38.* 已锁定的概要文件示例

场景	结果
概要文件 A 已锁定。它是使用密钥库 A 创建的。 概要文件 B 同样是使用密钥库 A 创建的。	概要文件 B 将被自动锁定。
概要文件 A 已创建并已启用。	概要文件 A 将被自动锁定。
概要文件 A、概要文件 B 和概要文件 C 当前已锁定。这些概要文件都是使用密钥库 A 创建的。 概要文件 B 已被选中并已单击**锁定/解锁**。	概要文件 A、概要文件 B 和概要文件 C 将被全部解锁。

数据模糊处理表达式

模糊处理表达式可识别要隐藏的数据。您可以根据基于字段的属性或使用正则表达式来创建模糊处理表达式。

基于字段的属性

使用基于字段的属性来隐藏用户名、组名、主机名和 NetBIOS 名称。使用基于字段的属性的表达式会对数据字符串的所有实例进行模糊处理。该数据将隐藏，而与其日志源、日志源类型、事件名称或事件类别无关。

如果在多个字段内存在相同数据值，那么会在包含该数据的所有字段中对该数据进行模糊处理，即使您已将概要文件配置为仅对四个字段中的一个字段进行模糊处理也是如此。例如，如果您有一个主机名称为 `IBMHost` 并且组名称为 `IBMHost`，那么在主机名字段和组名字段中都会对 `IBMHost` 的值进行模糊处理，即使数据模糊处理概要文件已配置为仅对主机名进行模糊处理也是如此。

正则表达式

使用正则表达式来对有效内容中的某个数据字符串进行模糊处理。仅当数据匹配表达式中定义的日志源、日志源类型、事件名称或类别时，才会隐藏该数据。

您可使用高级类别和低级类别来创建比基于字段的属性更具体的正则表达式。例如，您可使用以下正则表达式模式来解析用户名：

表 *39.* 正则表达式用户名解析

正则表达式模式示例	匹配
`usrName=([0-9a-zA-Z]([-.\w]*[0-9a-zA-Z])*@([0-9a-zA-Z][-\w]*[0-9a-zA-Z]\.)+[a-zA-Z]{2,20})$`	`john_smith@EXAMPLE.com, jon@example.com,jon@us.example.com`

表 39. 正则表达式用户名解析 (续)

正则表达式模式示例	匹配
`usrName=(^([\w]+[^\W])([^\W]\.?)([\w]+[^\W]$))`	john.smith, John.Smith, john, jon_smith
`usrName=^([a-zA-Z])[a-zA-Z_-]*[\w_-]*[\S]$\|^([a-zA-Z])[0-9_-]*[\S]$|^[a-zA-Z]*[\S]$`	johnsmith, Johnsmith123, john_smith123, john123_smith, john-smith
`usrName=(/S+)`	匹配等号 = 后的任意非空白字符。此正则表达式为非具体表达式，可能导致系统性能出现问题。
`msg=([0-9a-zA-Z]([-.\w]*[0-9a-zA-Z]))*@\b(([01]?\d?\d|2[0-4]\d|25[0-5])\.){3}([01]?\d?\d|2[0-4]\d|25[0-5])\b`	将用户与 IP 地址匹配。例如，john.smith@192.0.2.0
`src=\b(([01]?\d?\d|2[0-4]\d|25[0-5])\.){3}([01]?\d?\d|2[0-4]\d|25[0-5])\b`	匹配 IP 地址格式。
`host=^(([a-zA-Z0-9]|[a-zA-Z0-9][a-zA-Z0-9\-]*[a-zA-Z0-9])\.)*([A-Za-z0-9]|[A-Za-z0-9][A-Za-z0-9\-]*[A-Za-z0-9])$`	hostname.example.com, hostname.co.uk

场景：对用户名进行模糊处理

您是一名 IBM QRadar 管理员。您的组织与工会具有协议，必须对 QRadar 用户隐藏所有个人可标识信息。您想要将 QRadar 配置为隐藏所有用户名。

使用**管理**选项卡上的**数据模糊处理管理**功能来将 QRadar 配置为隐藏数据：

1. 创建数据模糊处理概要文件并下载系统生成的专用密钥。将密钥保存在安全位置。
2. 以您要隐藏的数据为目标创建数据模糊处理表达式。
3. 启用概要文件以便系统开始对数据进行模糊处理。
4. 要读取 QRadar 中的数据，请上载专用密钥以取消对数据进行的模糊处理。

创建数据模糊处理概要文件

IBM QRadar 使用数据模糊处理概要文件确定要屏蔽的数据，确保使用了正确密钥库取消屏蔽数据。

关于此任务

您可以创建可创建新密钥库的概要文件，或可使用现有密钥库。如果创建密钥库，那么必须下载并将其存储到安全位置。从本地系统移除密钥库，并将其存储到仅可由有权查看未屏蔽数据的用户访问的位置。

希望将数据访问权限制给不同用户组时，配置使用不同密钥库的概要文件会很有用。例如，希望一个用户组查看用户名，而另一个用户组查看主机名时，创建使用两个不同密钥库的概要文件。

过程

1. 在导航菜单（☰）上，单击**管理**。
2. 在**数据源**部分中单击**数据模糊处理管理**。
3. 要创建新的概要文件，请单击**添加**，并输入概要文件的唯一名称和描述。
4. 要为概要文件创建新的密钥库，请完成下列步骤：
   a) 单击**系统生成密钥库**。

b) 在**提供者**列表框中，选择 **IBMJCE**。

c) 在**算法**列表框中，选择 **JCE**，并选择生成 512 位还是 1024 位加密密钥。
在**密钥库证书 CN** 框中，会自动填充 QRadar 服务器的标准域名。

d) 在**密钥库密码**框中，输入密钥库密码。
密钥库密码用于保护密钥库的完整性。密码长度必须至少为 8 个字符。

e) 在**验证密钥库密码**中，再次输入密码。

5. 要将现有密钥库与概要文件配合使用，请完成下列步骤：

a) 单击**上载密钥库**。

b) 单击**浏览**并选择密钥库文件。

c) 在**密钥库密码**框中，输入密钥库密码。

6. 单击**提交**。
7. 下载密钥库。
从系统中移除密钥库并将其存储在安全位置。

下一步做什么

创建数据模糊处理表达式，这些表达式目标为要隐藏的数据。

创建数据模糊处理表达式

数据模糊处理概要文件使用表达式指定从 IBM QRadar 用户隐藏的数据。表达式可使用基于字段的属性或正则表达式。

关于此任务

在创建表达式后，您无法更改类型。例如，无法创建基于属性的表达式，然后将其更改为正则表达式。

无法隐藏规范化数字字段，例如，端口号或 IP 地址。

如果具有多个表达式隐藏相同数据，则会导致隐藏数据两次。要对多次隐藏的数据进行解密，必须按照之前模糊处理的顺序应用在模糊处理过程中使用的每个密钥库。

过程

1. 在导航菜单（☰）上，单击**管理**。
2. 在**数据源**部分中单击**数据模糊处理管理**。
3. 单击要配置的概要文件，并单击**查看内容**。
无法配置锁定的概要文件。
4. 要创建新的数据模糊处理表达式，请单击**添加**，并输入概要文件的唯一名称和描述。
5. 选中**已启用**复选框以启用概要文件。
6. 可选： 要将模糊处理表达式应用于特定域或租户，请从**域**字段进行选择。或者选择**所有域**以将模糊处理表达式应用于所有域和租户。
7. 要创建基于字段的表达式，请单击**基于字段**并选择要模糊处理的字段类型。
8. 要创建正则表达式，请单击**正则表达式**并配置正则表达式属性。
9. 单击**保存**。

取消模糊处理数据以使其可在控制台中进行查看

在 IBM QRadar 系统上配置了数据模糊处理时，会通过应用程序显示数据的屏蔽版本。必须同时具有对数据进行取消模糊处理的相应密钥库和密码，才可查看数据。

开始之前

您必须是管理员并且具有专用密钥和密钥的密码，才可对数据取消模糊处理。专用密钥必须位于本地计算机上。

关于此任务

在可查看模糊处理的数据之前，必须上载专用密钥。密钥上载后，当前会话时间段内，在系统上将保持可用。会话会在以下情况下结束：您从 QRadar 注销；在 QRadar Console 上清除了高速缓存；会话长时间不活动。会话结束时，在先前会话中上载的专用密钥不再可见。

QRadar 可以使用当前会话中可用的密钥，自动对数据取消模糊处理。启用了自动取消模糊处理时，您在每次查看数据时，不需要重复选择“**模糊处理会话密钥**”上的专用密钥。当前会话结束时，会自动禁用自动取消模糊处理。

过程

1. 在**事件详细信息**页面上，查找希望取消模糊处理的数据。
2. 要取消模糊处理基于身份的数据：
   a) 单击要取消模糊处理的数据旁的锁定图标。
   b) 在**上载密钥**部分中，单击**选择文件**并选择要上载的密钥库。
   c) 在**密码**框中，输入与密钥库匹配的密码。
   d) 单击**上载**。

      “**取消模糊处理**”窗口显示与密钥库、模糊处理的文本和取消模糊处理的文本关联的事件有效内容和概要文件名称。
   e) 可选： 单击**切换自动取消模糊处理**以启用自动取消模糊处理。

      切换自动取消模糊处理设置后，必须刷新浏览器窗口，并重新装入事件详细信息页面以显示更改。
3. 要取消模糊处理非基于身份的有效内容数据：
   a) 在**事件详细信息**页面的工具栏上，单击**模糊处理 > 取消模糊处理密钥**。
   b) 在**上载密钥**部分中，单击**选择文件**并选择要上载的专用密钥。
   c) 在**密码**框中，输入与专用密钥匹配的密码，并单击**上载**。
   d) 在**有效内容信息**框中，选择模糊处理的文本并将其复制到剪贴板。
   e) 在**事件详细信息**页面的工具栏上，单击**模糊处理 > 取消模糊处理**。
   f) 将模糊处理的文本粘贴到对话框中。
   g) 从下拉列表选择模糊处理概要文件，并单击**取消模糊处理**。

第 20 章 事件类别

事件类别用于分组传入事件以供 IBM QRadar 进行处理。事件类别可搜索且可帮助您监视网络。

网络中发生的事件会聚集到高级别和低级别的类别中。每个高级别类别均包含低级别类别，以及相关联的严重性级别和标识号。

您可以查看分配给事件的严重性级别并进行调整以适合公司政策需求。

您可以使用高级别和低级别事件类别标识来运行 AQL 查询。可以从事件类别表检索关联的类别名称的类别标识。

例如，如果在 QRadar 上开发应用程序，那么可以从命令行运行类似于以下查询的 AQL 搜索，以从 Ariel 收集数据：

```
select qidname(qid) as 'Event', username as 'Username', devicetime as 'Time'
from events where '<high-level category ID>' and '<Low-level category ID>' and
LOGSOURCENAME(logsourceid) like "%Low-level category name%" last 3 days
```

相关概念

IBM QRadar 产品中的功能

高级别事件类别

IBM QRadar 日志源中的事件分组到高级别类别。每个事件都分配一个特定高级类别。

对传入事件进行分类确保您可以轻松地搜索数据。

下表描述高级别事件类别。

表 *40.* 高级别事件类别

Category	类别标识	描述
第 146 页的『搜索』	1000	与扫描相关的事件以及用于标识网络资源的其他技术，例如，网络或主机端口扫描。
第 147 页的『DoS』	2000	与针对服务或主机的拒绝服务 (DoS) 或分布式拒绝服务 (DDoS) 攻击相关的事件，例如，暴力网络 DoS 攻击。
第 149 页的『认证』	3000	与认证控制、组或特权更改相关的事件，例如，登录或注销。
第 154 页的『访问』	4000	从尝试访问网络资源生成的事件，例如，防火墙接受或拒绝。
第 156 页的『利用』	5000	与应用程序渗透和缓冲区溢出尝试相关的事件，例如，缓冲区溢出或 Web 应用程序渗透。
第 157 页的『恶意软件』	6000	与病毒、特洛伊木马、后门攻击或其他形式的恶意软件相关的事件。恶意软件事件可能包括病毒、特洛伊木马、恶意软件或间谍软件。
第 158 页的『可疑活动』	7000	威胁性质未知但行为可疑。威胁可能包括可能指示规避技术的协议异常，例如，包分割或已知的侵入检测系统 (IDS) 规避技术。
第 161 页的『系统』	8000	与系统更改、软件安装或状态消息相关的事件。
第 164 页的『策略』	9000	有关公司政策违例或误用的事件。
第 165 页的『未知』	10000	有关系统上未知活动的事件。

表 40. 高级别事件类别 (续)		
Category	**类别标识**	**描述**
第 166 页的『CRE』	12000	从攻击或事件规则生成的事件。
第 166 页的『潜在利用』	13000	与潜在应用程序渗透和缓冲区溢出尝试相关的事件。
流	14000	与流操作相关的事件。
第 168 页的『由用户定义』	15000	与用户定义的对象相关的事件。
第 170 页的『SIM 审计』	16000	与控制台和管理功能的用户交互相关的事件。
第 171 页的『VIS 主机发现』	17000	与 VIS 组件发现的主机、端口或漏洞相关的事件。
第 171 页的『应用程序』	18000	与应用程序活动相关的事件。
第 190 页的『审计』	19000	与审计活动相关的事件。
第 192 页的『控制』	22000	与硬件系统相关的事件。
第 193 页的『资产概要分析程序』	23000	与资产概要文件相关的事件。
感应	24000	与 UBA 相关的事件。

搜索

侦察类别包含与扫描和用于识别网络资源的其他技术相关的事件。

下表描述侦察类别的低级别事件类别和关联的严重性级别。

表 41. 侦察事件类别的低级别类别和严重性级别			
低级别事件类别	**类别标识**	**描述**	**严重性级别 (0 - 10)**
未知的侦察形式	1001	未知形式的侦察。	2
应用程序查询	1002	侦察系统上的应用程序。	3
主机查询	1003	侦察网络中的主机。	3
网络扫描	1004	侦察网络。	4
邮件侦察	1005	侦察邮件系统。	3
Windows 侦察	1006	侦察 Windows 操作系统。	3
端口映射/RPC 请求	1007	侦察端口映射或 RPC 请求。	3
主机端口扫描	1008	指示在主机端口上发生扫描。	4
RPC 转储	1009	指示移除远程过程调用 (RPC) 信息。	3
DNS 侦察	1010	侦察 DNS 服务器。	3
其他侦察事件	1011	其他侦察事件。	2
Web 侦察	1012	网络上的 Web 侦察。	3

表 41. 侦察事件类别的低级别类别和严重性级别 (续)			
低级别事件类别	**类别标识**	**描述**	**严重性级别 (0 - 10)**
数据库侦察	1013	网络上的数据库侦察。	3
ICMP 侦察	1014	侦察 ICMP 流量。	3
UDP 侦察	1015	侦察 UDP 流量。	3
SNMP 侦察	1016	侦察 SNMP 流量。	3
ICMP 主机查询	1017	指示 ICMP 主机查询。	3
UDP 主机查询	1018	指示 UDP 端口查询。	3
NMAP 侦察	1019	指示 NMAP 侦察。	3
TCP 侦察	1020	指示网络上的 TCP 侦察。	3
UNIX 侦察	1021	侦察 UNIX 网络。	3
FTP 侦察	1022	指示 FTP 侦察。	3

DoS

DoS 类别包含与针对服务或主机的拒绝服务 (DoS) 攻击相关的事件。

下表描述了 DoS 类别的低级事件类别和关联的严重性级别。

表 42. DoS 事件类别的低级类别和严重性级别			
低级别事件类别	**类别标识**	**描述**	**严重性级别 (0 - 10)**
未知的 DoS 攻击	2001	指示未知的 DoS 攻击。	8
ICMP DoS	2002	指示 ICMP DoS 攻击。	9
TCP DoS	2003	指示 TCP DoS 攻击。	9
UDP DoS	2004	指示 UDP DoS 攻击。	9
DNS 服务 DoS	2005	指示 DNS 服务 DoS 攻击。	8
Web service DoS	2006	指示 Web 服务 DoS 攻击。	8
邮件服务 DoS	2007	指示邮件服务器 DoS 攻击。	8
分布式 DoS	2008	指示分布式 DoS 攻击。	9
其他 DoS	2009	指示其他 DoS 攻击。	8
UNIX DoS	2010	指示 UNIX DoS 攻击。	8
Windows DoS	2011	指示 Windows DoS 攻击。	8
数据库 DoS	2012	指示数据库 DoS 攻击。	8
FTP DoS	2013	指示 FTP DoS 攻击。	8
基础结构 DoS	2014	指示针对基础结构的 DoS 攻击。	8

表 *42. DoS* 事件类别的低级类别和严重性级别 *(续)*

低级别事件类别	类别标识	描述	严重性级别 (0 - 10)
Telnet DoS	2015	指示 Telnet DoS 攻击。	8
强行登录	2016	指示通过未经授权的方法访问您的系统。	8
高速率 TCP DoS	2017	指示高速率 TCP DoS 攻击。	8
高速率 UDP DoS	2018	指示高速率 UDP DoS 攻击。	8
高速率 ICMP DoS	2019	指示高速率 ICMP DoS 攻击。	8
高速率 DoS	2020	指示高速率 DoS 攻击。	8
中速率 TCP DoS	2021	指示中速率 TCP 攻击。	8
中速率 UDP DoS	2022	指示中速率 UDP 攻击。	8
中速率 ICMP DoS	2023	指示中速率 ICMP 攻击。	8
中速率 DoS	2024	指示中速率 DoS 攻击。	8
低速率 TCP DoS	2025	指示低速率 TCP DoS 攻击。	8
低速率 UDP DoS	2026	指示低速率 UDP DoS 攻击。	8
低速率 ICMP DoS	2027	指示低速率 ICMP DoS 攻击。	8
低速率 DoS	2028	指示低速率 DoS 攻击。	8
分布式高速率 TCP DoS	2029	指示分布式高速率 TCP DoS 攻击。	8
分布式高速率 UDP DoS	2030	指示分布式高速率 UDP DoS 攻击。	8
分布式高速率 ICMP DoS	2031	指示分布式高速率 ICMP DoS 攻击。	8
分布式高速率 DoS	2032	指示分布式高速率 DoS 攻击。	8
分布式中速率 TCP DoS	2033	指示分布式中速率 TCP DoS 攻击。	8
分布式中速率 UDP DoS	2034	指示分布式中速率 UDP DoS 攻击。	8
分布式中速率 ICMP DoS	2035	指示分布式中速率 ICMP DoS 攻击。	8
分布式中速率 DoS	2036	指示分布式中速率 DoS 攻击。	8
分布式低速率 TCP DoS	2037	指示分布式低速率 TCP DoS 攻击。	8

表 *42. DoS* 事件类别的低级类别和严重性级别 *(续)*

低级别事件类别	类别标识	描述	严重性级别 (0 - 10)
分布式低速率 UDP DoS	2038	指示分布式低速率 UDP DoS 攻击。	8
分布式低速率 ICMP DoS	2039	指示分布式低速率 ICMP DoS 攻击。	8
分布式低速率 DoS	2040	指示分布式低速率 DoS 攻击。	8
高速率 TCP 扫描	2041	指示高速率 TCP 扫描。	8
高速率 UDP 扫描	2042	指示高速率 UDP 扫描。	8
高速率 ICMP 扫描	2043	指示高速率 ICMP 扫描。	8
高速率扫描	2044	指示高速率扫描。	8
中速率 TCP 扫描	2045	指示中速率 TCP 扫描。	8
中速率 UDP 扫描	2046	指示中速率 UDP 扫描。	8
中速率 ICMP 扫描	2047	指示中速率 ICMP 扫描。	8
中速率扫描	2048	指示中速率扫描。	8
低速率 TCP 扫描	2049	指示低速率 TCP 扫描。	8
低速率 UDP 扫描	2050	指示低速率 UDP 扫描。	8
低速率 ICMP 扫描	2051	指示低速率 ICMP 扫描。	8
低速率扫描	2052	指示低速率扫描。	8
VoIP DoS	2053	指示 VoIP DoS 攻击。	8
洪流	2054	指示洪流攻击。	8
TCP 流量	2055	指示 TCP 洪流攻击。	8
UDP 流量	2056	指示 UDP 洪流攻击。	8
ICMP 流量	2057	指示 ICMP 洪流攻击。	8
SYN 流量	2058	指示 SYN 洪流攻击。	8
URG 流量	2059	指示含紧急 (URG) 标记的洪流攻击。	8
SYN URG 流量	2060	指示含紧急 (URG) 标记的 SYN 洪流攻击。	8
SYN FIN 流量	2061	指示 SYN FIN 洪流攻击。	8
SYN ACK 流量	2062	指示 SYN ACK 洪流攻击。	8

认证

认证类别包含与用于监视网络上的用户的认证、会话和访问控制相关的事件。

下表描述了认证类别的低级事件类别和关联的严重性级别。

表 *43.* 认证事件类别的低级类别和严重性级别

低级别事件类别	**类别标识**	**描述**	**严重性级别 (0 - 10)**
未知的认证	3001	指示未知认证。	1
主机登录成功	3002	指示主机登录成功。	1
主机登录失败	3003	指示主机登录失败。	3
其他登录成功	3004	指示登录序列成功。	1
其他登录失败	3005	指示登录序列失败。	3
特权升级失败	3006	指示特权升级失败。	3
特权升级成功	3007	指示特权升级成功。	1
邮件服务登录成功	3008	指示邮件服务登录成功。	1
邮件服务登录失败	3009	指示邮件服务登录失败。	3
认证服务器登录失败	3010	指示认证服务器登录失败。	3
认证服务器登录成功	3011	指示认证服务器登录成功。	1
Web service 登录成功	3012	指示 Web Service 登录成功。	1
Web service 登录失败	3013	指示 Web Service 登录失败。	3
管理员登录成功	3014	指示管理员登录成功。	1
管理员登录失败	3015	指示管理员登录失败。	3
可疑的用户名	3016	指示用户已尝试使用错误的用户名访问网络。	4
使用缺省用户名/密码登录成功	3017	指示用户已使用缺省用户名和密码访问网络。	4
使用缺省用户名/密码登录失败	3018	指示用户使用缺省用户名和密码访问网络失败。	4
FTP 登录成功	3019	指示 FTP 登录成功。	1
FTP 登录失败	3020	指示 FTP 登录失败。	3
SSH 登录成功	3021	指示 SSH 登录成功。	1
SSH 登录失败	3022	指示 SSH 登录失败。	2
已分配用户权限	3023	指示已成功授予用户对网络资源的访问权。	1
已移除用户权限	3024	指示已成功移除用户对网络资源的访问权。	1
已添加可信域	3025	指示可信域已成功添加到部署。	1
已移除可信域	3026	指示已从部署中移除可信域。	1
已授予系统安全性访问权	3027	指示已成功授予系统安全性访问权。	1

表 *43.* 认证事件类别的低级类别和严重性级别 *(续)*

低级别事件类别	类别标识	描述	严重性级别 (0 - 10)
已移除系统安全性访问权	3028	指示已成功移除系统安全性访问权。	1
已添加策略	3029	指示已成功添加策略。	1
策略更改	3030	指示已成功更改策略。	1
已添加用户帐户	3031	指示已成功添加用户帐户。	1
已更改用户帐户	3032	指示更改现有用户帐户。	1
密码更改失败	3033	指示尝试更改现有密码失败。	3
密码更改成功	3034	指示密码更改成功。	1
已移除用户帐户	3035	指示已成功移除用户帐户。	1
已添加组成员	3036	指示已成功添加组成员。	1
已移除组成员	3037	指示已移除组成员。	1
已添加组	3038	指示已成功添加组。	1
已更改组	3039	指示更改现有组。	1
已移除组	3040	指示已移除组。	1
已添加计算机帐户	3041	指示已成功添加计算机帐户。	1
已更改计算机帐户	3042	指示更改现有计算机帐户。	1
已移除计算机帐户	3043	指示已成功移除计算机帐户。	1
远程访问登录成功	3044	指示已成功使用远程登录访问网络。	1
远程访问登录失败	3045	指示尝试使用远程登录访问网络失败。	3
常规认证成功	3046	指示验证流程已成功。	1
常规认证失败	3047	指示认证流程失败。	3
Telnet 登录成功	3048	指示 telnet 登录成功。	1
Telnet 登录失败	3049	指示 telnet 登录失败。	3
可疑的密码	3050	指示用户尝试使用可疑密码进行登录。	4
Samba 登录成功	3051	指示用户已成功使用 Samba 登录。	1
Samba 登录失败	3052	指示用户使用 Samba 登录失败。	3
认证服务器会话已打开	3053	指示与认证服务器的通信会话已开始。	1

表 *43.* 认证事件类别的低级类别和严重性级别 *(续)*

低级别事件类别	类别标识	描述	严重性级别 (0 - 10)
认证服务器会话已关闭	3054	指示与认证服务器的通信会话已关闭。	1
防火墙会话已关闭	3055	指示防火墙会话已关闭。	1
主机注销	3056	指示主机已成功注销。	1
其他注销	3057	指示用户已成功注销。	1
认证服务器注销	3058	指示注销认证服务器的流程已成功。	1
Web service 注销	3059	指示注销 Web Service 的流程已成功。	1
管理员注销	3060	指示管理用户已成功注销。	1
FTP 注销	3061	指示注销 FTP 服务的流程已成功。	1
SSH 注销	3062	指示注销 SSH 会话的流程已成功。	1
远程访问注销	3063	指示使用远程访问注销的流程已成功。	1
Telnet 注销	3064	指示注销 Telnet 会话的流程已成功。	1
Samba 注销	3065	指示注销 Samba 的流程已成功。	1
SSH 会话已开始	3066	指示在主机上 SSH 登录会话已启动。	1
SSH 会话已结束	3067	指示在主机上 SSH 登录会话已终止。	1
Admin 会话已开始	3068	指示管理员或特权用户已在主机上启动登录会话。	1
Admin 会话已结束	3069	指示管理员或特权用户已在主机上终止登录会话。	1
VoIP 登录成功	3070	指示 VoIP 服务登录成功。	1
VoIP 登录失败	3071	指示尝试访问 VoIP 服务失败。	1
VoIP 注销	3072	指示用户注销。	1
VoIP 会话已启动	3073	指示 VoIP 会话已开始。	1
VoIP 会话已终止	3074	指示 VoIP 会话已结束。	1
数据库登录成功	3075	指示数据库登录成功。	1
数据库登录失败	3076	指示数据库登录尝试失败。	3

表 *43.* 认证事件类别的低级类别和严重性级别 *(续)*

低级别事件类别	类别标识	描述	严重性级别 (0 - 10)
IKE 认证失败	3077	指示已检测到因特网密钥交换 (IKE) 认证失败。	3
IKE 认证成功	3078	指示已检测到 IKE 认证成功。	1
IKE 会话已开始	3079	指示 IKE 会话已开始。	1
IKE 会话已结束	3080	指示 IKE 会话已结束。	1
IKE 错误	3081	指示 IKE 错误消息。	1
IKE 状态	3082	指示 IKE 状态消息。	1
RADIUS 会话已开始	3083	指示 RADIUS 会话已开始。	1
RADIUS 会话已结束	3084	指示 RADIUS 会话已结束。	1
RADIUS 会话被拒绝	3085	指示 RADIUS 会话已遭拒绝。	1
RADIUS 会话状态	3086	指示 RADIUS 会话状态消息。	1
RADIUS 认证失败	3087	指示 RADIUS 认证失败。	3
RADIUS 认证成功	3088	指示 RADIUS 认证已成功。	1
TACACS 会话已开始	3089	指示 TACACS 会话已开始。	1
TACACS 会话已结束	3090	指示 TACACS 会话已结束。	1
TACACS 会话被拒绝	3091	指示 TACACS 会话已遭拒绝。	1
TACACS 会话状态	3092	指示 TACACS 会话状态消息。	1
TACACS 认证成功	3093	指示 TACACS 认证已成功。	1
TACACS 认证失败	3094	指示 TACACS 认证失败。	1
取消主机认证成功	3095	指示主机取消认证已成功。	1
取消主机认证失败	3096	指示主机取消认证失败。	3
站认证成功	3097	指示站认证已成功。	1
站认证失败	3098	指示主机的站认证失败。	3
站关联成功	3099	指示站关联已成功。	1
站关联失败	3100	指示站关联失败。	3
站重新关联成功	3101	指示站重新关联已成功。	1
站重新关联失败	3102	指示站关联失败。	3

表 43. 认证事件类别的低级类别和严重性级别 (续)

低级别事件类别	类别标识	描述	严重性级别 (0 - 10)
取消主机关联成功	3103	指示主机取消关联已成功。	1
取消主机关联失败	3104	指示取消主机关联失败。	3
SA 错误	3105	指示安全性关联 (SA) 错误消息。	5
SA 创建失败	3106	指示安全性关联 (SA) 创建失败。	3
SA 已建立	3107	指示安全性关联 (SA) 连接已建立。	1
SA 被拒绝	3108	指示安全性关联 (SA) 连接遭拒绝。	3
正在删除 SA	3109	指示删除安全性关联 (SA)。	1
正在创建 SA	3110	指示创建安全性关联 (SA)。	1
证书不匹配	3111	指示证书不匹配。	3
凭证不匹配	3112	指示凭证不匹配。	3
管理员登录尝试	3113	指示管理员登录尝试。	2
用户登录尝试	3114	指示用户登录尝试。	2
用户登录成功	3115	指示用户登录成功。	1
用户登录失败	3116	指示用户登录失败。	3
SFTP 登录成功	3117	指示 SSH 文件传输协议 (SFTP) 登录成功。	1
SFTP 登录失败	3118	指示 SSH 文件传输协议 (SFTP) 登录失败。	3
SFTP 注销	3119	指示 SSH 文件传输协议 (SFTP) 注销。	1
已授予身份	3120	指示已授予身份。	1
已移除身份	3121	指示已移除身份。	1
已撤销身份	3122	指示已撤销身份。	1
已移除策略	3123	指示已移除策略。	1
用户帐户锁定	3124	指示已锁定用户帐户。	1
用户帐户解锁	3125	指示已解除用户帐户锁定	1
用户帐户已到期	3126	指示用户帐户已到期	1

访问

访问类别包含用于监视网络事件的认证和访问控制。

下表描述了访问类别的低级事件类别和关联的严重性级别。

表 *44.* 访问事件类别的低级类别和严重性级别

低级别事件类别	**类别标识**	**描述**	**严重性级别 (0 - 10)**
未知的网络通信事件	4001	指示未知网络通信事件。	3
防火墙许可	4002	指示已允许访问防火墙。	0
拒绝通过防火墙	4003	指示已拒绝访问防火墙。	4
流上下文响应（仅限 QRadar SIEM）	4004	指示来自“分类引擎”的旨在响应 SIM 请求的事件。	5
其他网络通信事件	4005	指示其他通信事件。	3
IPS 拒绝	4006	指示入侵防御系统 (IPS) 拒绝的流量。	4
防火墙会话已打开	4007	指示防火墙会话已打开。	0
防火墙会话已关闭	4008	指示防火墙会话已关闭。	0
动态地址转换成功	4009	指示动态地址转换成功。	0
找不到任何转换组	4010	指示找不到任何转换组。	2
其他授权	4011	指示已授予对其他认证服务器的访问权。	2
ACL 许可	4012	指示访问控制表 (ACL) 允许的访问。	0
ACL 拒绝	4013	指示访问控制表 (ACL) 拒绝的访问。	4
访问获准	4014	指示已允许访问。	0
访问遭拒绝	4015	指示访问已遭拒绝。	4
会话已打开	4016	指示会话已打开。	1
会话已关闭	4017	指示会话已关闭。	1
会话已重置	4018	指示会话已重置。	3
会话已终止	4019	指示已允许会话。	4
会话被拒绝	4020	指示会话已遭拒绝。	5
会话正在进行中	4021	指示正在进行会话。	1
会话已延迟	4022	指示会话已延迟。	3
会话已排队	4023	指示会话已入队。	1
会话入站	4024	指示会话已入站。	1
会话出站	4025	指示会话已出站。	1
未经授权的访问尝试	4026	指示检测到未经授权的访问尝试。	6
允许其他应用程序操作	4027	指示已允许应用程序操作。	1
拒绝其他应用程序操作	4028	指示应用程序操作已遭拒绝。	3

表 44. 访问事件类别的低级类别和严重性级别 (续)			
低级别事件类别	**类别标识**	**描述**	**严重性级别 (0 - 10)**
允许数据库操作	4029	指示已允许数据库操作。	1
拒绝数据库操作	4030	指示数据库操作已遭拒绝。	3
允许 FTP 操作	4031	指示已允许 FTP 操作。	1
拒绝 FTP 操作	4032	指示 FTP 操作已遭拒绝。	3
已高速缓存对象	4033	指示已缓存对象。	1
未高速缓存对象	4034	指示未缓存对象。	1
速率限制	4035	指示网络对流量进行速率限制。	4
无速率限制	4036	指示网络不对流量进行速率限制。	0
允许 P11 访问	4037	指示允许 P11 访问。	8
P11 访问遭拒绝	4038	指示已尝试 P11 访问，但遭拒绝。	8
IPS 许可	4039	指示 IPS 许可。	0

利用

渗透类别包含发生通信或访问渗透的事件。

下表描述渗透类别的低级别事件类别和关联的严重性级别。

表 45. 渗透事件类别的低级别类别和严重性级别			
低级别事件类别	**类别标识**	**描述**	**严重性级别 (0 - 10)**
未知的渗透攻击	5001	指示未知的渗透攻击。	9
缓冲区溢出	5002	指示缓冲区溢出。	9
DNS 渗透	5003	指示 DNS 渗透。	9
Telnet 渗透	5004	指示 Telnet 渗透。	9
Linux 渗透	5005	指示 Linux 渗透。	9
UNIX 渗透	5006	指示 UNIX 渗透。	9
Windows 渗透	5007	指示 Microsoft Windows 渗透。	9
邮件渗透	5008	指示邮件服务器渗透。	9
基础结构渗透	5009	指示基础结构渗透。	9
其他渗透	5010	指示杂项渗透。	9
Web 渗透	5011	指示 Web 渗透。	9
会话劫持	5012	指示网络中的会话被拦截。	9

表 45. 渗透事件类别的低级别类别和严重性级别 (续)			
低级别事件类别	**类别标识**	**描述**	**严重性级别 (0 - 10)**
蠕虫处于活动状态	5013	指示活动的蠕虫。	10
密码猜测/检索	5014	指示用户请求访问数据库中的密码信息。	9
FTP 渗透	5015	指示 FTP 渗透。	9
RPC 渗透	5016	指示 RPC 渗透。	9
SNMP 渗透	5017	指示 SNMP 渗透。	9
空操作渗透	5018	指示空操作渗透。	9
Samba 渗透	5019	指示 Samba 渗透。	9
SSH 渗透	5020	指示 SSH 渗透。	9
数据库渗透	5021	指示数据库渗透。	9
ICMP 渗透	5022	指示 ICMP 渗透。	9
UDP 渗透	5023	指示 UDP 渗透。	9
浏览器渗透	5024	指示浏览器上的渗透。	9
DHCP 渗透	5025	指示 DHCP 渗透	9
远程访问渗透	5026	指示远程访问渗透	9
ActiveX 利用	5027	指示通过 ActiveX 应用程序的渗透。	9
SQL 注入	5028	指示发生了 SQL 注入。	9
跨站点脚本编制	5029	指示跨站点脚本编制漏洞。	9
格式字符串漏洞	5030	指示格式字符串漏洞。	9
输入验证利用	5031	指示检测到输入验证渗透尝试。	9
远程代码执行	5032	指示检测到远程代码执行尝试。	9
内存损坏	5033	指示检测到内存损坏渗透。	9
命令执行	5034	指示检测到远程命令执行尝试。	9
代码注入	5035	指示检测到代码注入。	9
重放攻击	5036	指示检测到重放攻击。	9

恶意软件

恶意软件 (malware) 类别包含与应用程序渗透和缓冲区溢出尝试相关的事件。

下表描述恶意软件类别的低级别事件类别和关联的严重性级别。

表 46. 恶意软件事件类别的低级别类别和严重性级别

低级别事件类别	类别标识	描述	严重性级别 (0 - 10)
未知的恶意软件	6001	指示未知病毒。	4
检测到后门	6002	指示检测到系统后门。	9
不怀好意的邮件附件	6003	指示不怀好意的邮件附件。	6
恶意软件	6004	指示病毒。	6
不怀好意的软件下载	6005	指示到网络的不怀好意的软件下载。	6
检测到病毒	6006	指示检测到病毒。	8
其他恶意软件	6007	指示其他恶意软件	4
检测到木马	6008	指示检测到木马。	7
检测到间谍软件	6009	指示在系统上检测到间谍软件。	6
内容扫描	6010	指示检测到内容扫描尝试。	3
内容扫描失败	6011	指示内容扫描失败。	8
内容扫描成功	6012	指示内容扫描成功。	3
内容扫描正在进行	6013	指示内容扫描正在进行中。	3
键记录器	6014	指示检测到键记录器。	7
检测到恶意广告软件	6015	指示检测到恶意广告软件。	4
隔离成功	6016	指示隔离操作已成功完成。	3
隔离失败	6017	指示隔离操作失败。	8
恶意软件感染	6018	指示检测到恶意软件感染。	10
移除成功	6019	指示移除成功。	3
移除失败	6020	指示移除失败。	8

可疑活动

可疑类别包含与病毒、特洛伊木马、后门攻击和其他形式的恶意软件相关的事件。

下表描述可疑活动类别的低级别事件类别和关联的严重性级别。

表 47. 可疑活动事件类别的低级别类别和严重性级别

低级别事件类别	类别标识	描述	严重性级别 (0 - 10)
未知的可疑事件	7001	指示未知的可疑事件。	3
检测到可疑的模式	7002	指示检测到可疑的模式。	3
防火墙已修改内容	7003	指示防火墙修改了内容。	3

表 47. 可疑活动事件类别的低级别类别和严重性级别 (续)

低级别事件类别	类别标识	描述	严重性级别 (0 - 10)
无效的命令或数据	7004	指示命令或数据无效。	3
可疑的包	7005	指示可疑的包。	3
可疑活动	7006	指示可疑活动。	3
可疑的文件名	7007	指示可疑的文件名。	3
可疑的端口活动	7008	指示可疑的端口活动。	3
可疑的路由	7009	指示可疑的路由。	3
潜在 Web 漏洞	7010	指示潜在 Web 漏洞。	3
未知的规避事件	7011	指示未知的规避事件。	5
IP 仿冒	7012	指示 IP 仿冒。	5
IP 分段	7013	指示 IP 分段。	3
重叠的 IP 片段	7014	指示重叠的 IP 分段。	5
IDS 规避	7015	指示 IDS 规避。	5
DNS 协议异常	7016	指示 DNS 协议异常。	3
FTP 协议异常	7017	指示 FTP 协议异常。	3
邮件协议异常	7018	指示邮件协议异常。	3
路由协议异常	7019	指示路由协议异常。	3
Web 协议异常	7020	指示 Web 协议异常。	3
SQL 协议异常	7021	指示 SQL 协议异常。	3
检测到可执行代码	7022	指示检测到可执行代码。	5
其他可疑事件	7023	指示其他可疑事件。	3
信息泄漏	7024	指示信息泄漏。	1
潜在邮件漏洞	7025	指示邮件服务器中的潜在漏洞。	4
潜在版本漏洞	7026	指示 IBM QRadar 版本中的潜在漏洞。	4
潜在 FTP 漏洞	7027	指示潜在 FTP 漏洞。	4
潜在 SSH 漏洞	7028	指示潜在 SSH 漏洞。	4
潜在 DNS 漏洞	7029	指示 DNS 服务器中的潜在漏洞。	4
潜在 SMB 漏洞	7030	指示潜在 SMB (Samba) 漏洞。	4
潜在数据库漏洞	7031	指示数据库中的潜在漏洞。	4
IP 协议异常	7032	指示潜在 IP 协议异常。	3
可疑的 IP 地址	7033	指示检测到可疑的 IP 地址。	2

表 47. 可疑活动事件类别的低级别类别和严重性级别 (续)

低级别事件类别	类别标识	描述	严重性级别 (0 - 10)
无效的 IP 协议使用	7034	指示 IP 协议无效。	2
无效的协议	7035	指示协议无效。	4
可疑的窗口事件	7036	指示桌面屏幕上的可疑事件。	2
可疑的 ICMP 活动	7037	指示可疑的 ICMP 活动。	2
潜在 NFS 漏洞	7038	指示潜在网络文件系统 (NFS) 漏洞。	4
潜在 NNTP 漏洞	7039	指示潜在网络新闻传输协议 (NNTP) 漏洞。	4
潜在 RPC 漏洞	7040	指示潜在 RPC 漏洞。	4
潜在 Telnet 漏洞	7041	指示系统上的潜在 Telnet 漏洞。	4
潜在 SNMP 漏洞	7042	指示潜在 SNMP 漏洞。	4
非法的 TCP 标志组合	7043	指示检测到无效的 TCP 标志组合。	5
可疑的 TCP 标志组合	7044	指示检测到潜在的无效 TCP 标志组合。	4
非法的 ICMP 协议使用	7045	指示检测到 ICMP 协议的无效使用。	5
可疑的 ICMP 协议使用	7046	指示检测到 ICMP 协议的潜在无效使用。	4
非法的 ICMP 类型	7047	指示检测到无效的 ICMP 类型。	5
非法的 ICMP 代码	7048	指示检测到无效的 ICMP 代码。	5
可疑的 ICMP 类型	7049	指示检测到潜在无效的 ICMP 类型。	4
可疑的 ICMP 代码	7050	指示检测到潜在无效的 ICMP 代码。	4
TCP 端口 0	7051	指示 TCP 包将保留端口 (0) 用于源或目标。	4
UDP 端口 0	7052	指示 UDP 包将保留端口 (0) 用于源或目标。	4
不怀好意的 IP	7053	指示使用了已知不怀好意的 IP 地址。	4
监测列表 IP	7054	指示使用了来自 IP 地址监测列表的 IP 地址。	4
已知攻击者 IP	7055	指示使用了已知攻击者的 IP 地址。	4
RFC 1918（专用）IP	7056	指示使用了来自专用 IP 地址范围的 IP 地址。	4

表 47. 可疑活动事件类别的低级别类别和严重性级别 (续)			
低级别事件类别	**类别标识**	**描述**	**严重性级别 (0 - 10)**
潜在的 VoIP 漏洞	7057	指示潜在的 VoIP 漏洞。	4
黑名单地址	7058	指示 IP 地址位于黑名单上。	8
监测列表地址	7059	指示 IP 地址位于要监视的 IP 地址列表上。	7
暗网地址	7060	指示 IP 地址属于暗网。	5
僵尸网络地址	7061	指示地址属于僵尸网络。	7
可疑地址	7062	指示必须监视 IP 地址。	5
不良内容	7063	指示检测到不良内容。	7
证书无效	7064	指示检测到无效证书。	7
用户活动	7065	指示检测到用户活动。	7
可疑的协议使用	7066	指示检测到可疑的协议使用。	5
可疑的 BGP 活动	7067	指示检测到可疑的边界网关协议 (BGP) 使用。	5
路由中毒	7068	指示检测到路由损坏。	5
ARP 中毒	7069	指示检测到 ARP 高速缓存中毒。	5
检测到流氓设备	7070	指示检测到流氓设备。	5
政府机构地址	7071	指示检测到政府机构地址。	3

系统

系统类别包含与系统更改、软件安装或状态消息相关的事件。

下表描述系统类别的低级别事件类别和关联的严重性级别。

表 48. 系统事件类别的低级别类别和严重性级别			
低级别事件类别	**类别标识**	**描述**	**严重性级别 (0 - 10)**
未知的系统事件	8001	指示未知的系统事件。	1
系统引导	8002	指示系统重新启动。	1
系统配置	8003	指示系统配置更改。	1
系统暂停	8004	指示系统已暂停。	1
系统故障	8005	指示系统故障。	6
系统状态	8006	指示任何信息事件。	1
系统错误	8007	指示系统错误。	3
其他系统事件	8008	指示其他系统事件。	1
服务已启动	8009	指示系统服务已启动。	1

表 *48.* 系统事件类别的低级别类别和严重性级别 *(续)*

低级别事件类别	类别标识	描述	严重性级别 (0 - 10)
服务已停止	8010	指示系统服务已停止。	1
服务失败	8011	指示系统故障。	6
注册表修改成功	8012	指示注册表修改已成功。	1
主机策略修改成功	8013	指示主机策略修改已成功。	1
文件修改成功	8014	指示文件修改已成功。	1
堆栈修改成功	8015	指示堆栈修改已成功。	1
应用程序修改成功	8016	指示应用程序修改已成功。	1
配置修改成功	8017	指示配置修改已成功。	1
服务修改成功	8018	指示服务修改已成功。	1
注册表修改失败	8019	指示注册表修改失败。	1
主机策略修改失败	8020	指示主机策略修改失败。	1
文件修改失败	8021	指示文件修改失败。	1
堆栈修改失败	8022	指示堆栈修改失败。	1
应用程序修改失败	8023	指示应用程序修改失败。	1
配置修改失败	8024	指示配置修改失败。	1
服务修改失败	8025	指示服务修改失败。	1
注册表添加	8026	指示已向注册表添加新项。	1
已创建主机策略	8027	指示已向注册表添加新条目。	1
文件已创建	8028	指示在系统中创建了新文件。	1
已安装应用程序	8029	指示在系统上安装了新应用程序。	1
已安装服务	8030	指示在系统上安装了新服务。	1
注册表删除	8031	指示已删除注册表条目。	1
已删除主机策略	8032	指示已删除主机策略条目。	1
文件已删除	8033	指示已删除文件。	1
已卸载应用程序	8034	指示已卸载应用程序。	1
已卸载服务	8035	指示已卸载服务。	1
系统参考	8036	指示系统信息。	3
系统操作允许	8037	指示已授权系统上尝试的操作。	3

表 *48.* 系统事件类别的低级别类别和严重性级别 *(续)*

低级别事件类别	类别标识	描述	严重性级别 (0 - 10)
系统操作拒绝	8038	指示已拒绝系统上尝试的操作。	4
Cron	8039	指示 crontab 消息。	1
Cron 状态	8040	指示 crontab 状态消息。	1
Cron 失败	8041	指示 crontab 失败消息。	4
Cron 成功	8042	指示 crontab 成功消息。	1
守护程序	8043	指示守护程序消息。	1
守护程序状态	8044	指示守护程序状态消息。	1
守护程序失败	8045	指示守护程序失败消息。	4
守护程序成功	8046	指示守护程序成功消息。	1
内核	8047	指示内核消息。	1
内核状态	8048	指示内核状态消息。	1
内核失败	8049	指示内核失败消息。	
内核成功	8050	指示内核成功消息。	1
认证	8051	指示认证消息。	1
信息	8052	指示参考消息。	2
通知	8053	指示通知消息。	3
警告	8054	指示警告消息。	5
错误	8055	指示错误消息。	7
严重	8056	指示严重消息。	9
调试	8057	指示调试消息。	1
消息	8058	指示一般消息。	1
特权访问	8059	指示尝试了特权访问。	3
警报	8060	指示警报消息。	9
紧急	8061	指示紧急消息。	9
SNMP 状态	8062	指示 SNMP 状态消息。	1
FTP 状态	8063	指示 FTP 状态消息。	1
NTP 状态	8064	指示 NTP 状态消息。	1
访问点无线故障	8065	指示访问点无线故障。	3
加密协议配置不匹配	8066	指示加密协议配置不匹配。	3
客户机设备或认证服务器配置错误	8067	指示未正确配置客户机设备或认证服务器。	5
热备用启用失败	8068	指示热备用启用失败。	5
热备用禁用失败	8069	指示热备用禁用失败。	5

表 48. 系统事件类别的低级别类别和严重性级别 (续)			
低级别事件类别	**类别标识**	**描述**	**严重性级别 (0 - 10)**
热备用已成功启用	8070	指示已成功启用热备用。	1
热备用关联丢失	8071	指示热备用关联丢失。	5
MainMode 启动失败	8072	指示 MainMode 启动失败。	5
MainMode 启动已成功	8073	指示 MainMode 启动已成功。	1
MainMode 状态	8074	指示已报告 MainMode 状态消息。	1
快速模式启动失败	8075	指示快速模式启动失败。	5
快速模式启动成功	8076	指示快速模式启动已成功。	1
快速模式状态	8077	指示已报告快速模式状态消息。	1
许可证无效	8078	指示许可证无效。	3
许可证已到期	8079	指示许可证已到期。	3
已应用新的许可证	8080	指示已应用新许可证。	1
许可证错误	8081	指示许可证错误。	5
许可证状态	8082	指示许可证状态消息。	1
配置错误	8083	指示检测到配置错误。	5
服务中断	8084	指示检测到服务中断。	5
已超过 EPS 或 FPM 分配	8085	指示已超过 EPS 或 FPM 的许可证池分配。	3
性能状态	8086	指示已报告性能状态。	1
性能下降	8087	指示性能下降。	4
配置错误	8088	指示检测到不正确的配置。	5

策略

策略类别包含与网络策略的管理和策略违例的监视网络资源相关的事件。

下表描述策略类别的低级别事件类别和关联的严重性级别。

表 49. 策略类别的低级别类别和严重性级别			
低级别事件类别	**类别标识**	**描述**	**严重性级别 (0 - 10)**
未知的策略违例	9001	指示未知策略违例。	2
Web 策略违例	9002	指示 Web 策略违例。	2
远程访问策略违例	9003	指示远程访问策略违例。	2
IRC/IM 策略违例	9004	指示即时通讯策略违例。	2

表 *49.* 策略类别的低级别类别和严重性级别 *(续)*			
低级别事件类别	**类别标识**	**描述**	**严重性级别 (0 - 10)**
P2P 策略违例	9005	指示对等 (P2P) 策略违例。	2
IP 访问策略违例	9006	指示 IP 访问策略违例。	2
应用程序策略违例	9007	指示应用程序策略违例。	2
数据库策略违例	9008	指示数据库策略违例。	2
网络阈值策略违例	9009	指示网络阈值策略违例。	2
色情策略违例	9010	指示色情策略违例。	2
游戏策略违例	9011	指示游戏策略违例。	2
其他策略违例	9012	指示其他策略违例。	2
合规性策略违例	9013	指示合规性策略违例。	2
邮件策略违例	9014	指示邮件策略违例。	2
IRC 策略违例	9015	指示 IRC 策略违例	2
IM 策略违例	9016	指示与即时消息 (IM) 活动相关的策略违例。	2
VoIP 策略违例	9017	指示 VoIP 策略违例	2
已成功	9018	指示策略成功消息。	1
已失败	9019	指示策略失败消息。	4
数据丢失预防策略违例	9020	指示数据丢失预防策略违例。	2
监测列表对象	9021	指示监测列表对象。	2
允许 Web 策略	9022	指示允许新的 Web 策略。	1

未知

“未知”类别包含未解析并因此无法分类的事件。

下表描述“未知”类别的低级别事件类别和关联的严重性级别。

表 *50.* “未知”类别的低级别类别和严重性级别			
低级别事件类别	**类别标识**	**描述**	**严重性级别 (0 - 10)**
未知	10001	指示未知事件。	3
未知的 Snort 事件	10002	指示未知 Snort 事件。	3
未知的 Dragon 事件	10003	指示未知 Dragon 事件。	3
未知的 Pix 防火墙事件	10004	指示未知 Cisco 私有因特网交换 (PIX) 防火墙 事件。	3
未知的 Tipping Point 事件	10005	指示未知 HP TippingPoint 事件。	3

表 50. “未知”类别的低级别类别和严重性级别 (续)			
低级别事件类别	**类别标识**	**描述**	**严重性级别 (0 - 10)**
未知 Windows 认证服务器事件	10006	指示未知 Windows Auth Server 事件。	3
未知的 Nortel 事件	10007	指示未知 Nortel 事件。	3
存储	10009	指示未知存储事件。	3
行为	11001	指示未知行为事件。	3
阈值	11002	指示未知阈值事件。	3
异常	11003	指示未知异常事件。	3

CRE

定制规则事件 (CRE) 类别包含从定制攻击、流或事件规则生成的事件。

下表描述了 CRE 类别的低级事件类别和关联的严重性级别。

表 51. *CRE* 类别的低级类别和严重性级别			
低级别事件类别	**类别标识**	**描述**	**严重性级别 (0 - 10)**
未知的 CRE 事件	12001	指示未知定制规则引擎事件。	5
单事件规则匹配	12002	指示单一事件规则匹配。	5
事件序列规则匹配	12003	指示事件序列规则匹配。	5
交叉攻击事件序列规则匹配	12004	指示交叉攻击事件序列规则匹配。	5
攻击规则匹配	12005	指示攻击规则匹配。	5

潜在利用

潜在渗透类别包含与潜在应用程序渗透和缓冲区溢出尝试相关的事件。

下表描述潜在渗透类别的低级别事件类别和关联的严重性级别。

表 52. 潜在渗透类别的低级别类别和严重性级别			
低级别事件类别	**类别标识**	**描述**	**严重性级别 (0 - 10)**
未知的潜在渗透攻击	13001	指示检测到潜在渗透攻击。	7
潜在缓冲区溢出	13002	指示检测到潜在缓冲区溢出。	7
潜在的 DNS 渗透	13003	指示检测到通过 DNS 服务器的潜在渗透攻击。	7
潜在的 Telnet 渗透	13004	指示检测到通过 Telnet 的潜在渗透攻击。	7
潜在 Linux 渗透	13005	指示检测到通过 Linux 的潜在渗透攻击。	7

表 52. 潜在渗透类别的低级别类别和严重性级别 (续)			
低级别事件类别	**类别标识**	**描述**	**严重性级别 (0 - 10)**
潜在 UNIX 渗透	13006	指示检测到通过 UNIX 的潜在渗透攻击。	7
潜在 Windows 渗透	13007	指示检测到通过 Windows 的潜在渗透攻击。	7
潜在的邮件渗透	13008	指示检测到通过邮件的潜在渗透攻击。	7
潜在的基础结构渗透	13009	指示在系统基础结构上检测到潜在渗透攻击。	7
潜在的其他渗透	13010	指示检测到潜在渗透攻击。	7
潜在的 Web 渗透	13011	指示检测到通过 Web 的潜在渗透攻击。	7
潜在的僵尸网络连接	13012	指示检测到使用僵尸网络的潜在渗透攻击。	6
潜在的蠕虫活动	13013	指示检测到使用蠕虫活动的潜在攻击。	6

流

流类别包含与流操作相关的事件。

下表描述流类别的低级别事件类别和关联的严重性级别。

表 53. 流类别的低级别类别和严重性级别			
低级别事件类别	**类别标识**	**描述**	**严重性级别 (0 - 10)**
单向流	14001	指示事件的单向流。	5
单向流数量少	14002	指示事件的单向流数量少。	5
单向流数量中等	14003	指示事件的单向流数量中等。	5
单向流数量多	14004	指示事件的单向流数量多。	5
单向 TCP 流	14005	指示单向 TCP 流。	5
单向 TCP 流数量少	14006	指示单向 TCP 流数量少。	5
单向 TCP 流数量中等	14007	指示单向 TCP 流数量中等。	5
单向 TCP 流数量多	14008	指示单向 TCP 流数量多。	5
单向 ICMP 流	14009	指示单向 ICMP 流。	5
单向 ICMP 流数量少	14010	指示单向 ICMP 流数量少。	5
单向 ICMP 流数量中等	14011	指示单向 ICMP 流数量中等。	5
单向 ICMP 流数量多	14012	指示单向 ICMP 流数量多。	5
可疑的 ICMP 流	14013	指示可疑的 ICMP 流。	5
可疑的 UDP 流	14014	指示可疑的 UDP 流。	5

表 53. 流类别的低级别类别和严重性级别 (续)			
低级别事件类别	**类别标识**	**描述**	**严重性级别 (0 - 10)**
可疑的 TCP 流	14015	指示可疑的 TCP 流。	5
可疑流	14016	指示可疑流。	5
空包流	14017	指示空包流。	5
空包流数量少	14018	指示空包流数量少。	5
空包流数量中等	14019	指示空包流数量中等。	5
空包流数量多	14020	指示空包流数量多。	5
大型有效内容流	14021	指示大型有效内容流。	5
大型有效内容流数量少	14022	指示大型有效内容流数量少。	5
大型有效内容流数量中等	14023	指示大型有效内容流数量中等。	5
大型有效内容流数量多	14024	指示大型有效内容流数量多。	5
一个攻击者攻击多个目标流	14025	指示一个攻击者攻击多个流。	5
多个攻击者攻击一个目标流	14026	指示多个攻击者攻击一个流。	5
未知流	14027	指示未知流。	5
Netflow 记录	14028	指示 Netflow 记录。	5
QFlow 记录	14029	指示 QFlow 记录。	5
SFlow 记录	14030	指示 SFlow 记录。	5
Packeteer 记录	14031	指示 Packeteer 记录。	5
其他流	14032	指示其他流。	5
大数据传输	14033	指示大数据传输。	5
大数据传输出站	14034	指示大数据出站传输。	5
VoIP 流	14035	指示 VoIP 流。	5

由用户定义

用户定义的类别包含与用户定义的对象相关的事件

下表描述用户定义的类别的低级别事件类别和关联的严重性级别。

表 54. 用户定义的类别的低级别类别和严重性级别			
低级别事件类别	**类别标识**	**描述**	**严重性级别 (0 - 10)**
定制 Sentry 低	15001	指示低严重性定制异常事件。	3
定制 Sentry 中等	15002	指示中等严重性定制异常事件。	5
定制 Sentry 高	15003	指示高严重性定制异常事件。	7

表 *54.* 用户定义的类别的低级别类别和严重性级别 *(续)*

低级别事件类别	类别标识	描述	严重性级别 (0 - 10)
定制 Sentry 1	15004	指示严重性级别为 1 的定制异常事件。	1
定制 Sentry 2	15005	指示严重性级别为 2 的定制异常事件。	2
定制 Sentry 3	15006	指示严重性级别为 3 的定制异常事件。	3
定制 Sentry 4	15007	指示严重性级别为 4 的定制异常事件。	4
定制 Sentry 5	15008	指示严重性级别为 5 的定制异常事件。	5
定制 Sentry 6	15009	指示严重性级别为 6 的定制异常事件。	6
定制 Sentry 7	15010	指示严重性级别为 7 的定制异常事件。	7
定制 Sentry 8	15011	指示严重性级别为 8 的定制异常事件。	8
定制 Sentry 9	15012	指示严重性级别为 9 的定制异常事件。	9
定制策略低	15013	指示具有低严重性级别的定制策略事件。	3
定制策略中等	15014	指示具有中等严重性级别的定制策略事件。	5
定制策略高	15015	指示具有高严重性级别的定制策略事件。	7
定制策略 1	15016	指示严重性级别为 1 的定制策略事件。	1
定制策略 2	15017	指示严重性级别为 2 的定制策略事件。	2
定制策略 3	15018	指示严重性级别为 3 的定制策略事件。	3
定制策略 4	15019	指示严重性级别为 4 的定制策略事件。	4
定制策略 5	15020	指示严重性级别为 5 的定制策略事件。	5
定制策略 6	15021	指示严重性级别为 6 的定制策略事件。	6
定制策略 7	15022	指示严重性级别为 7 的定制策略事件。	7
定制策略 8	15023	指示严重性级别为 8 的定制策略事件。	8
定制策略 9	15024	指示严重性级别为 9 的定制策略事件。	9

表 54. 用户定义的类别的低级别类别和严重性级别 (续)

低级别事件类别	类别标识	描述	严重性级别 (0 - 10)
定制用户低	15025	指示具有低严重性级别的定制用户事件。	3
定制用户中等	15026	指示具有中等严重性级别的定制用户事件。	5
定制用户高	15027	指示具有高严重性级别的定制用户事件。	7
定制用户 1	15028	指示严重性级别为 1 的定制用户事件。	1
定制用户 2	15029	指示严重性级别为 2 的定制用户事件。	2
定制用户 3	15030	指示严重性级别为 3 的定制用户事件。	3
定制用户 4	15031	指示严重性级别为 4 的定制用户事件。	4
定制用户 5	15032	指示严重性级别为 5 的定制用户事件。	5
定制用户 6	15033	指示严重性级别为 6 的定制用户事件。	6
定制用户 7	15034	指示严重性级别为 7 的定制用户事件。	7
定制用户 8	15035	指示严重性级别为 8 的定制用户事件。	8
定制用户 9	15036	指示严重性级别为 9 的定制用户事件。	9

SIM 审计

SIM 审计类别包含与 IBM QRadar 控制台和管理功能的用户交互相关的事件。

下表描述 SIM 审计类别的低级别事件类别和关联的严重性级别。

表 55. *SIM* 审计类别的低级别类别和严重性级别

低级别事件类别	类别标识	描述	严重性级别 (0 - 10)
SIM 用户认证	16001	指示控制台上的用户登录或注销。	5
SIM 配置更改	16002	指示用户更改了 SIM 配置或部署。	3
SIM 用户操作	16003	指示用户在 SIM 模块启动了过程，例如，启动备份或生成报告。	3
会话已创建	16004	指示已创建用户会话。	3
会话已销毁	16005	指示已销毁用户会话。	3

表 55. SIM 审计类别的低级别类别和严重性级别 (续)			
低级别事件类别	**类别标识**	**描述**	**严重性级别 (0 - 10)**
Admin 会话已创建	16006	指示已创建 Admin 会话。	
Admin 会话已销毁	16007	指示已销毁 Admin 会话。	3
会话认证无效	16008	指示无效的会话认证。	5
会话认证已到期	16009	指示会话认证已到期。	3
风险管理器配置	16010	指示用户已更改 IBM QRadar Risk Manager 配置。	3

VIS 主机发现

当 VIS 组件发现并存储网络上检测到的新主机、端口漏洞时，VIS 组件会生成事件。这些事件发送到 事件收集器 以与其他安全事件关联。

下表描述 VIS 主机发现类别的低级别事件类别和关联的严重性级别。

表 56. VIS 主机发现类别的低级别类别和严重性级别			
低级别事件类别	**类别标识**	**描述**	**严重性级别 (0 - 10)**
已发现新主机	17001	指示 VIS 组件检测到新主机。	3
已发现新端口	17002	指示 VIS 组件检测到新的打开端口。	3
已发现新漏洞	17003	指示 VIS 组件检测到新漏洞。	3
已发现新操作系统	17004	指示 VIS 组件在主机上检测到新操作系统。	3
已发现批量主机	17005	指示 VIS 组件在短期内检测到许多新主机。	3

应用程序

应用程序类别包含与应用程序活动相关的事件，如电子邮件或 FTP 活动。

下表描述了应用程序类别的低级事件类别和关联的严重性级别。

表 57. 应用程序类别的低级类别和严重性级别			
低级别事件类别	**类别标识**	**描述**	**严重性级别 (0 - 10)**
邮件已打开	18001	指示电子邮件连接已建立。	1
邮件已关闭	18002	指示电子邮件连接已关闭。	1
邮件已重置	18003	指示电子邮件连接已重置。	3

表 57. 应用程序类别的低级类别和严重性级别 (续)

低级别事件类别	类别标识	描述	严重性级别 (0 - 10)
邮件已终止	18004	指示电子邮件连接已终止。	4
邮件被拒绝	18005	指示电子邮件连接已遭拒绝。	4
正在发送邮件	18006	指示正在尝试建立电子邮件连接。	1
邮件已延迟	18007	指示电子邮件连接已延迟。	4
邮件已排队	18008	指示电子邮件连接已入队。	3
邮件已重定向	18009	指示电子邮件连接已重定向。	1
FTP 已打开	18010	指示 FTP 连接已处于打开状态。	1
FTP 已关闭	18011	指示 FTP 连接已关闭。	1
FTP 已重置	18012	指示 FTP 连接已重置。	3
FTP 已终止	18013	指示 FTP 连接已终止。	4
FTP 被拒绝	18014	指示 FTP 连接已遭拒绝。	4
FTP 正在进行中	18015	指示正在进行 FTP 连接。	1
FTP 已重定向	18016	指示 FTP 连接已重定向。	3
HTTP 已打开	18017	指示 HTTP 连接已建立。	1
HTTP 已关闭	18018	指示 HTTP 连接已关闭。	1
HTTP 已重置	18019	指示 HTTP 连接已重置。	3
HTTP 已终止	18020	指示 HTTP 连接已终止。	4
HTTP 被拒绝	18021	指示 HTTP 连接已遭拒绝。	4
HTTP 正在进行中	18022	指示正在进行 HTTP 连接。	1
HTTP 已延迟	18023	指示 HTTP 连接已延迟。	3
HTTP 已排队	18024	指示 HTTP 连接已入队。	1
HTTP 已重定向	18025	指示 HTTP 连接已重定向。	1
HTTP 代理	18026	指示要通过代理建立的 HTTP 连接。	1
HTTPS 已打开	18027	指示 HTTPS 连接已建立。	1

表 57. 应用程序类别的低级类别和严重性级别 (续)

低级别事件类别	类别标识	描述	严重性级别 (0 - 10)
HTTPS 已关闭	18028	指示 HTTPS 连接已关闭。	1
HTTPS 已重置	18029	指示 HTTPS 连接已重置。	3
HTTPS 已终止	18030	指示 HTTPS 连接已终止。	4
HTTPS 被拒绝	18031	指示 HTTPS 连接已遭拒绝。	4
HTTPS 正在进行中	18032	指示正在进行 HTTPS 连接。	1
HTTPS 已延迟	18033	指示 HTTPS 连接已延迟。	3
HTTPS 已排队	18034	指示 HTTPS 连接已入队。	3
HTTPS 已重定向	18035	指示 HTTPS 连接已重定向。	3
HTTPS 代理	18036	指示已通过代理建立 HTTPS 连接。	1
SSH 已打开	18037	指示 SSH 连接已建立。	1
SSH 已关闭	18038	指示 SSH 连接已关闭。	1
SSH 已重置	18039	指示 SSH 连接已重置。	3
SSH 已终止	18040	指示 SSH 连接已终止。	4
SSH 被拒绝	18041	指示 SSH 会话已遭拒绝。	4
SSH 正在进行中	18042	指示正在进行 SSH 会话。	1
RemoteAccess 已打开	18043	指示远程访问连接已建立。	1
RemoteAccess 已关闭	18044	指示远程访问连接已关闭。	1
RemoteAccess 已重置	18045	指示远程访问连接已重置。	3
RemoteAccess 已终止	18046	指示远程访问连接已终止。	4
RemoteAccess 被拒绝	18047	指示远程访问连接已遭拒绝。	4
RemoteAccess 正在进行中	18048	指示正在进行远程访问连接。	1
RemoteAccess 已延迟	18049	指示远程访问连接已延迟。	3

表 57. 应用程序类别的低级类别和严重性级别 (续)

低级别事件类别	类别标识	描述	严重性级别 (0 - 10)
RemoteAccess 已重定向	18050	指示远程访问连接已重定向。	3
VPN 已打开	18051	指示 VPN 连接已处于打开状态。	1
VPN 已关闭	18052	指示 VPN 连接已关闭。	1
VPN 已重置	18053	指示 VPN 连接已重置。	3
VPN 已终止	18054	指示 VPN 连接已终止。	4
VPN 被拒绝	18055	指示 VPN 连接已遭拒绝。	4
VPN 正在进行中	18056	指示正在进行 VPN 连接。	1
VPN 已延迟	18057	指示 VPN 连接已延迟。	3
VPN 已排队	18058	指示 VPN 连接已入队。	3
VPN 已重定向	18059	指示 VPN 连接已重定向。	3
RDP 已打开	18060	指示 RDP 连接已建立。	1
RDP 已关闭	18061	指示 RDP 连接已关闭。	1
RDP 已重置	18062	指示 RDP 连接已重置。	3
RDP 已终止	18063	指示 RDP 连接已终止。	4
RDP 被拒绝	18064	指示 RDP 连接已遭拒绝。	4
RDP 正在进行中	18065	指示正在进行 RDP 连接。	1
RDP 已重定向	18066	指示 RDP 连接已重定向。	3
FileTransfer 已打开	18067	指示文件传输连接已建立。	1
FileTransfer 已关闭	18068	指示文件传输连接已关闭。	1
FileTransfer 已重置	18069	指示文件传输连接已重置。	3
FileTransfer 已终止	18070	指示文件传输连接已终止。	4
FileTransfer 被拒绝	18071	指示文件传输连接已遭拒绝。	4
FileTransfer 正在进行中	18072	指示正在进行文件传输连接。	1
FileTransfer 已延迟	18073	指示文件传输连接已延迟。	3

表 57. 应用程序类别的低级类别和严重性级别 (续)

低级别事件类别	类别标识	描述	严重性级别 (0 - 10)
FileTransfer 已排队	18074	指示文件传输连接已入队。	3
FileTransfer 已重定向	18075	指示文件传输连接已重定向。	3
DNS 已打开	18076	指示 DNS 连接已建立。	1
DNS 已关闭	18077	指示 DNS 连接已关闭。	1
DNS 已重置	18078	指示 DNS 连接已重置。	5
DNS 已终止	18079	指示 DNS 连接已终止。	5
DNS 被拒绝	18080	指示 DNS 连接已遭拒绝。	5
DNS 正在进行中	18081	指示正在进行 DNS 连接。	1
DNS 已延迟	18082	指示 DNS 连接已延迟。	5
DNS 已重定向	18083	指示 DNS 连接已重定向。	4
聊天已打开	18084	指示聊天连接已处于打开状态。	1
聊天已关闭	18085	指示聊天连接已关闭。	1
聊天已重置	18086	指示聊天连接已重置。	3
聊天已终止	18087	指示聊天连接已终止。	3
聊天被拒绝	18088	指示聊天连接已遭拒绝。	3
聊天正在进行中	18089	指示正在进行聊天连接。	1
聊天已重定向	18090	指示聊天连接已重定向。	1
数据库已打开	18091	指示数据库连接已建立。	1
数据库已关闭	18092	指示数据库连接已关闭。	1
数据库已重置	18093	指示数据库连接已重置。	5
数据库已终止	18094	指示数据库连接已终止。	5
数据库被拒绝	18095	指示数据库连接已遭拒绝。	5
数据库正在进行中	18096	指示正在进行数据库连接。	1
数据库已重定向	18097	指示数据库连接已重定向。	3
SMTP 已打开	18098	指示 SMTP 连接已建立。	1
SMTP 已关闭	18099	指示 SMTP 连接已关闭。	1
SMTP 已重置	18100	指示 SMTP 连接已重置。	3
SMTP 已终止	18101	指示 SMTP 连接已终止。	5

表 57. 应用程序类别的低级类别和严重性级别 (续)

低级别事件类别	类别标识	描述	严重性级别 (0 - 10)
SMTP 被拒绝	18102	指示 SMTP 连接已遭拒绝。	5
SMTP 正在进行中	18103	指示正在进行 SMTP 连接。	1
SMTP 已延迟	18104	指示 SMTP 连接已延迟。	3
SMTP 已排队	18105	指示 SMTP 连接已入队。	3
SMTP 已重定向	18106	指示 SMTP 连接已重定向。	3
认证已打开	18107	指示授权服务器连接已建立。	1
认证已关闭	18108	指示授权服务器连接已关闭。	1
认证已重置	18109	指示授权服务器连接已重置。	3
认证已终止	18110	指示授权服务器连接已终止。	4
认证被拒绝	18111	指示授权服务器连接已遭拒绝。	4
认证正在进行中	18112	指示正在进行授权服务器连接。	1
认证已延迟	18113	指示授权服务器连接已延迟。	3
认证已排队	18114	指示授权服务器连接已入队。	3
认证已重定向	18115	指示授权服务器连接已重定向。	2
P2P 已打开	18116	指示对等 (P2P) 连接已建立。	1
P2P 已关闭	18117	指示 P2P 连接已关闭。	1
P2P 已重置	18118	指示 P2P 连接已重置。	4
P2P 已终止	18119	指示 P2P 连接已终止。	4
P2P 被拒绝	18120	指示 P2P 连接已遭拒绝。	3
P2P 正在进行中	18121	指示正在进行 P2P 连接。	1
Web 已打开	18122	指示 Web 连接已建立。	1
Web 已关闭	18123	指示 Web 连接已关闭。	1
Web 已重置	18124	指示 Web 连接已重置。	4
Web 已终止	18125	指示 Web 连接已终止。	4

表 57. 应用程序类别的低级类别和严重性级别 (续)

低级别事件类别	类别标识	描述	严重性级别 (0 - 10)
Web 已拒绝	18126	指示 Web 连接已遭拒绝。	4
Web 正在进行中	18127	指示正在进行 Web 连接。	1
Web 已延迟	18128	指示 Web 连接已延迟。	3
Web 已排队	18129	指示 Web 连接已入队。	1
Web 已重定向	18130	指示 Web 连接已重定向。	1
Web 代理	18131	指示已通过代理建立 Web 连接。	1
VoIP 已打开	18132	指示 Voice Over IP (VoIP) 连接已建立。	1
VoIP 已关闭	18133	指示 VoIP 连接已关闭。	1
VoIP 已重置	18134	指示 VoIP 连接已重置。	3
VoIP 已终止	18135	指示 VoIP 连接已终止。	3
VoIP 被拒绝	18136	指示 VoIP 连接已遭拒绝。	3
VoIP 正在进行中	18137	指示正在进行 VoIP 连接。	1
VoIP 已延迟	18138	指示 VoIP 连接已延迟。	3
VoIP 已重定向	18139	指示 VoIP 连接已重定向。	3
LDAP 会话已开始	18140	指示 LDAP 会话已开始。	1
LDAP 会话已结束	18141	指示 LDAP 会话已结束。	1
LDAP 会话被拒绝	18142	指示 LDAP 会话已遭拒绝。	3
LDAP 会话状态	18143	指示已报告 LDAP 会话状态消息。	1
LDAP 认证失败	18144	指示 LDAP 认证失败。	4
LDAP 认证成功	18145	指示 LDAP 认证成功。	1
AAA 会话已开始	18146	指示已开始认证、授权和记帐 (AAA) 会话。	1
AAA 会话已结束	18147	指示 AAA 会话已结束。	1
AAA 会话被拒绝	18148	指示 AAA 会话已遭拒绝。	3
AAA 会话状态	18149	指示已报告 AAA 会话状态消息。	1
AAA 认证失败	18150	指示 AAA 认证失败。	4
AAA 认证成功	18151	指示 AAA 认证成功。	1

表 57. 应用程序类别的低级类别和严重性级别 (续)

低级别事件类别	类别标识	描述	严重性级别 (0 - 10)
IPSEC 认证失败	18152	指示因特网协议安全性 (IPSEC) 认证失败。	4
IPSEC 认证成功	18153	指示 IPSEC 认证成功。	1
IPSEC 会话已开始	18154	指示 IPSEC 会话已开始。	1
IPSEC 会话已结束	18155	指示 IPSEC 会话已结束。	1
IPSEC 错误	18156	指示已报告 IPSEC 错误消息。	5
IPSEC Status	18157	指示已报告 IPSEC 会话状态消息。	1
IM 会话已打开	18158	指示已建立即时消息 (IM) 会话。	1
IM 会话已关闭	18159	指示 IM 会话已关闭。	1
IM 会话已重置	18160	指示 IM 会话已重置。	3
IM 会话已终止	18161	指示 IM 会话已终止。	3
IM 会话被拒绝	18162	指示 IM 会话已遭拒绝。	3
IM 会话进行中	18163	指示正在进行 IM 会话。	1
IM 会话已延迟	18164	指示 IM 会话已延迟。	3
IM 会话已重定向	18165	指示 IM 会话已重定向。	3
WHOIS 会话已打开	18166	指示 WHOIS 会话已建立。	1
WHOIS 会话已关闭	18167	指示 WHOIS 会话已关闭。	1
WHOIS 会话已重置	18168	指示 WHOIS 会话已重置。	3
WHOIS 会话终止	18169	指示 WHOIS 会话已终止。	3
WHOIS 会话遭拒绝	18170	指示 WHOIS 会话已遭拒绝。	3
WHOIS 会话正在进行中	18171	指示正在进行 WHOIS 会话。	1
WHOIS 会话已重定向	18172	指示 WHOIS 会话已重定向。	3
Traceroute 会话已打开	18173	指示 Traceroute 会话已建立。	1
Traceroute 会话已关闭	18174	指示 Traceroute 会话已关闭。	1
Traceroute 会话被拒绝	18175	指示 Traceroute 会话已遭拒绝。	3

表 57. 应用程序类别的低级类别和严重性级别 (续)

低级别事件类别	类别标识	描述	严重性级别 (0 - 10)
Traceroute 会话正在进行中	18176	指示正在进行 Traceroute 会话。	1
TN3270 会话已打开	18177	TN3270 是一个终端仿真程序，用于连接至 IBM 3270 终端。此类别指示已建立 TN3270 会话。	1
TN3270 会话已关闭	18178	指示 TN3270 会话已关闭。	1
TN3270 会话已重置	18179	指示 TN3270 会话已重置。	3
TN3270 会话已终止	18180	指示 TN3270 会话已终止。	3
TN3270 会话被拒绝	18181	指示 TN3270 会话已遭拒绝。	3
TN3270 会话正在进行中	18182	指示正在进行 TN3270 会话。	1
TFTP 会话已打开	18183	指示 TFTP 会话已建立。	1
TFTP 会话已关闭	18184	指示 TFTP 会话已关闭。	1
TFTP 会话已重置	18185	指示 TFTP 会话已重置。	3
TFTP 会话已终止	18186	指示 TFTP 会话已终止。	3
TFTP 会话被拒绝	18187	指示 TFTP 会话已遭拒绝。	3
TFTP 会话正在进行中	18188	指示正在进行 TFTP 会话。	1
Telnet 会话已打开	18189	指示 Telnet 会话已建立。	1
Telnet 会话已关闭	18190	指示 Telnet 会话已关闭。	1
Telnet 会话已重置	18191	指示 Telnet 会话已重置。	3
Telnet 会话已终止	18192	指示 Telnet 会话已终止。	3
Telnet 会话被拒绝	18193	指示 Telnet 会话已遭拒绝。	3
Telnet 会话正在进行中	18194	指示正在进行 Telnet 会话。	1
Syslog 会话已打开	18201	指示 Syslog 会话已建立。	1
Syslog 会话已关闭	18202	指示 Syslog 会话已关闭。	1
Syslog 会话被拒绝	18203	指示 Syslog 会话已遭拒绝。	3

表 57. 应用程序类别的低级类别和严重性级别 (续)

低级别事件类别	类别标识	描述	严重性级别 (0 - 10)
Syslog 会话正在进行中	18204	指示正在进行 Syslog 会话。	1
SSL 会话已打开	18205	指示安全套接字层 (SSL) 会话已建立。	1
SSL 会话已关闭	18206	指示 SSL 会话已关闭。	1
SSL 会话已重置	18207	指示 SSL 会话已重置。	3
SSL 会话已终止	18208	指示 SSL 会话已终止。	3
SSL 会话被拒绝	18209	指示 Syslog 会话已遭拒绝。	3
SSL 会话正在进行中	18210	指示正在进行 SSL 会话。	1
SNMP 会话已打开	18211	指示简单网络管理协议 (SNMP) 会话已建立。	1
SNMP 会话已关闭	18212	指示 SNMP 会话已关闭。	1
SNMP 会话被拒绝	18213	指示 SNMP 会话已遭拒绝。	3
SNMP 会话正在进行中	18214	指示正在进行 SNMP 会话。	1
SMB 会话已打开	18215	指示服务器消息块 (SMB) 会话已建立。	1
SMB 会话已关闭	18216	指示 SMB 会话已关闭。	1
SMB 会话已重置	18217	指示 SMB 会话已重置。	3
SMB 会话已终止	18218	指示 SMB 会话已终止。	3
SMB 会话被拒绝	18219	指示 SMB 会话已遭拒绝。	3
SMB 会话正在进行中	18220	指示正在进行 SMB 会话。	1
流媒体会话已打开	18221	指示流媒体会话已建立。	1
流媒体会话已关闭	18222	指示流媒体会话已关闭。	1
流媒体会话已重置	18223	指示流媒体会话已重置。	3
流媒体会话已终止	18224	指示流媒体会话已终止。	3
流媒体会话被拒绝	18225	指示流媒体会话已遭拒绝。	3
流媒体会话正在进行中	18226	指示正在进行流媒体会话。	1
RUSERS 会话已打开	18227	指示 RUSERS（远程用户）会话已建立。	1
RUSERS 会话已关闭	18228	指示 RUSERS 会话已关闭。	1

表 57. 应用程序类别的低级类别和严重性级别 (续)

低级别事件类别	类别标识	描述	严重性级别 (0 - 10)
RUSERS 会话被拒绝	18229	指示 RUSERS 会话已遭拒绝。	3
RUSERS 会话正在进行中	18230	指示正在进行 RUSERS 会话。	1
Rsh 会话已打开	18231	指示远程 shell (rsh) 会话已建立。	1
Rsh 会话已关闭	18232	指示 rsh 会话已关闭。	1
Rsh 会话已重置	18233	指示 rsh 会话已重置。	3
Rsh 会话终止	18234	指示 rsh 会话已终止。	3
Rsh 会话遭拒绝	18235	指示 rsh 会话已遭拒绝。	3
Rsh 会话正在进行中	18236	指示正在进行 rsh 会话。	1
RLOGIN 会话已打开	18237	指示远程登录 (RLOGIN) 会话已建立。	1
RLOGIN 会话已关闭	18238	指示 RLOGIN 会话已关闭。	1
RLOGIN 会话已重置	18239	指示 RLOGIN 会话已重置。	3
RLOGIN 会话已终止	18240	指示 RLOGIN 会话已终止。	3
RLOGIN 会话被拒绝	18241	指示 RLOGIN 会话已遭拒绝。	3
RLOGIN 会话正在进行中	18242	指示正在进行 RLOGIN 会话。	1
REXEC 会话已打开	18243	指示 REXEC（远程执行）会话已建立。	1
REXEC 会话已关闭	18244	指示 REXEC 会话已关闭。	1
REXEC 会话已重置	18245	指示 REXEC 会话已重置。	3
REXEC 会话已终止	18246	指示 REXEC 会话已终止。	3
REXEC 会话被拒绝	18247	指示 REXEC 会话已遭拒绝。	3
REXEC 会话正在进行中	18248	指示正在进行 REXEC 会话。	1
RPC 会话已打开	18249	指示远程过程调用 (RPC) 会话已建立。	1
RPC 会话已关闭	18250	指示 RPC 会话已关闭。	1
RPC 会话已重置	18251	指示 RPC 会话已重置。	3
RPC 会话已终止	18252	指示 RPC 会话已终止。	3

表 57. 应用程序类别的低级类别和严重性级别 (续)

低级别事件类别	类别标识	描述	严重性级别 (0 - 10)
RPC 会话被拒绝	18253	指示 RPC 会话已遭拒绝。	3
RPC 会话正在进行中	18254	指示正在进行 RPC 会话。	1
NTP 会话已打开	18255	指示网络时间协议 (NTP) 会话已建立。	1
NTP 会话已关闭	18256	指示 NTP 会话已关闭。	1
NTP 会话已重置	18257	指示 NTP 会话已重置。	3
NTP 会话已终止	18258	指示 NTP 会话已终止。	3
NTP 会话被拒绝	18259	指示 NTP 会话已遭拒绝。	3
NTP 会话正在进行中	18260	指示正在进行 NTP 会话。	1
NNTP 会话已打开	18261	指示网络新闻传输协议 (NNTP) 会话已建立。	1
NNTP 会话已关闭	18262	指示 NNTP 会话已关闭。	1
NNTP 会话已重置	18263	指示 NNTP 会话已重置。	3
NNTP 会话已终止	18264	指示 NNTP 会话已终止。	3
NNTP 会话被拒绝	18265	指示 NNTP 会话已遭拒绝。	3
NNTP 会话正在进行中	18266	指示正在进行 NNTP 会话。	1
NFS 会话已打开	18267	指示网络文件系统 (NFS) 会话已建立。	1
NFS 会话已关闭	18268	指示 NFS 会话已关闭。	1
NFS 会话已重置	18269	指示 NFS 会话已重置。	3
NFS 会话已终止	18270	指示 NFS 会话已终止。	3
NFS 会话被拒绝	18271	指示 NFS 会话已遭拒绝。	3
NFS 会话正在进行中	18272	指示正在进行 NFS 会话。	1
NCP 会话已打开	18273	指示网络控制程序 (NCP) 会话已建立。	1
NCP 会话已关闭	18274	指示 NCP 会话已关闭。	1
NCP 会话已重置	18275	指示 NCP 会话已重置。	3
NCP 会话已终止	18276	指示 NCP 会话已终止。	3
NCP 会话被拒绝	18277	指示 NCP 会话已遭拒绝。	3

表 57. 应用程序类别的低级类别和严重性级别 (续)

低级别事件类别	类别标识	描述	严重性级别 (0 - 10)
NCP 会话正在进行中	18278	指示正在进行 NCP 会话。	1
NetBIOS 会话已打开	18279	指示 NetBIOS 会话已建立。	1
NetBIOS 会话已关闭	18280	指示 NetBIOS 会话已关闭。	1
NetBIOS 会话已重置	18281	指示 NetBIOS 会话已重置。	3
NetBIOS 会话已终止	18282	指示 NetBIOS 会话已终止。	3
NetBIOS 会话被拒绝	18283	指示 NetBIOS 会话已遭拒绝。	3
NetBIOS 会话正在进行中	18284	指示正在进行 NetBIOS 会话。	1
MODBUS 会话已打开	18285	指示 MODBUS 会话已建立。	1
MODBUS 会话已关闭	18286	指示 MODBUS 会话已关闭。	1
MODBUS 会话已重置	18287	指示 MODBUS 会话已重置。	3
MODBUS 会话已终止	18288	指示 MODBUS 会话已终止。	3
MODBUS 会话被拒绝	18289	指示 MODBUS 会话已遭拒绝。	3
MODBUS 会话正在进行中	18290	指示正在进行 MODBUS 会话。	1
LPD 会话已打开	18291	指示行式打印机守护程序 (LPD) 会话已建立。	1
LPD 会话已关闭	18292	指示 LPD 会话已关闭。	1
LPD 会话已重置	18293	指示 LPD 会话已重置。	3
LPD 会话已终止	18294	指示 LPD 会话已终止。	3
LPD 会话被拒绝	18295	指示 LPD 会话已遭拒绝。	3
LPD 会话正在进行中	18296	指示正在进行 LPD 会话。	1
Lotus Notes® 会话已打开	18297	指示 Lotus Notes 会话已建立。	1
Lotus Notes 会话已关闭	18298	指示 Lotus Notes 会话已关闭。	1
Lotus Notes 会话已重置	18299	指示 Lotus Notes 会话已重置。	3

表 57. 应用程序类别的低级类别和严重性级别 (续)

低级别事件类别	类别标识	描述	严重性级别 (0 - 10)
Lotus Notes 会话终止	18300	指示 Lotus Notes 会话已终止。	3
Lotus Notes 会话遭拒绝	18301	指示 Lotus Notes 会话已遭拒绝。	3
Lotus Notes 会话正在进行中	18302	指示正在进行 Lotus Notes 会话。	1
Kerberos 会话已打开	18303	指示 Kerberos 会话已建立。	1
Kerberos 会话已关闭	18304	指示 Kerberos 会话已关闭。	1
Kerberos 会话已重置	18305	指示 Kerberos 会话已重置。	3
Kerberos 会话已终止	18306	指示 Kerberos 会话已终止。	3
Kerberos 会话被拒绝	18307	指示 Kerberos 会话已遭拒绝。	3
Kerberos 会话正在进行中	18308	指示正在进行 Kerberos 会话。	1
IRC 会话已打开	18309	指示因特网中继设备聊天 (IRC) 会话已建立。	1
IRC 会话已关闭	18310	指示 IRC 会话已关闭。	1
IRC 会话已重置	18311	指示 IRC 会话已重置。	3
IRC 会话已终止	18312	指示 IRC 会话已终止。	3
IRC 会话被拒绝	18313	指示 IRC 会话已遭拒绝。	3
IRC 会话正在进行中	18314	指示正在进行 IRC 会话。	1
IEC 104 会话已打开	18315	指示 IEC 104 会话已建立。	1
IEC 104 会话已关闭	18316	指示 IEC 104 会话已关闭。	1
IEC 104 会话已重置	18317	指示 IEC 104 会话已重置。	3
IEC 104 会话已终止	18318	指示 IEC 104 会话已终止。	3
IEC 104 会话被拒绝	18319	指示 IEC 104 会话已遭拒绝。	3
IEC 104 会话正在进行中	18320	指示正在进行 IEC 104 会话。	1
Ident 会话已打开	18321	指示 TCP 客户机身份协议 (Ident) 会话已建立。	1
Ident 会话已关闭	18322	指示 Ident 会话已关闭。	1

表 57. 应用程序类别的低级类别和严重性级别 (续)

低级别事件类别	类别标识	描述	严重性级别 (0 - 10)
Ident 会话已重置	18323	指示 Ident 会话已重置。	3
Ident 会话已终止	18324	指示 Ident 会话已终止。	3
Ident 会话被拒绝	18325	指示 Ident 会话已遭拒绝。	3
Ident 会话正在进行中	18326	指示正在进行 Ident 会话。	1
ICCP 会话已打开	18327	指示控制中心间通信协议 (ICCP) 会话已建立。	1
ICCP 会话已关闭	18328	指示 ICCP 会话已关闭。	1
ICCP 会话已重置	18329	指示 ICCP 会话已重置。	3
ICCP 会话已终止	18330	指示 ICCP 会话已终止。	3
ICCP 会话被拒绝	18331	指示 ICCP 会话已遭拒绝。	3
ICCP 会话正在进行中	18332	指示正在进行 ICCP 会话。	1
GroupWise 会话已打开	18333	指示 GroupWise 会话已建立。	1
GroupWise 会话已关闭	18334	指示 GroupWise 会话已关闭。	1
GroupWise 会话已重置	18335	指示 GroupWise 会话已重置。	3
GroupWise 会话已终止	18336	指示 GroupWise 会话已终止。	3
GroupWiseSession Denied	18337	指示 GroupWise 会话已遭拒绝。	3
GroupWise 会话正在进行中	18338	指示正在进行 GroupWise 会话。	1
Gopher 会话已打开	183398	指示 Gopher 会话已建立。	1
Gopher 会话已关闭	18340	指示 Gopher 会话已关闭。	1
Gopher 会话已重置	18341	指示 Gopher 会话已重置。	3
Gopher 会话已终止	18342	指示 Gopher 会话已终止。	3
Gopher 会话被拒绝	18343	指示 Gopher 会话已遭拒绝。	3
Gopher 会话正在进行中	18344	指示正在进行 Gopher 会话。	1
GIOP 会话已打开	18345	指示通用 ORB 间协议 (GIOP) 会话已建立。	1

表 57. 应用程序类别的低级类别和严重性级别 (续)

低级别事件类别	类别标识	描述	严重性级别 (0 - 10)
GIOP 会话已关闭	18346	指示 GIOP 会话已关闭。	1
GIOP 会话已重置	18347	指示 GIOP 会话已重置。	3
GIOP 会话已终止	18348	指示 GIOP 会话已终止。	3
GIOP 会话被拒绝	18349	指示 GIOP 会话已遭拒绝。	3
GIOP 会话正在进行中	18350	指示正在进行 GIOP 会话。	1
Finger 会话已打开	18351	指示 Finger 会话已建立。	1
Finger 会话已关闭	18352	指示 Finger 会话已关闭。	1
Finger 会话已重置	18353	指示 Finger 会话已重置。	3
Finger 会话已终止	18354	指示 Finger 会话已终止。	3
Finger 会话被拒绝	18355	指示 Finger 会话已遭拒绝。	3
Finger 会话正在进行中	18356	指示正在进行 Finger 会话。	1
Echo 会话已打开	18357	指示 Echo 会话已建立。	1
Echo 会话已关闭	18358	指示 Echo 会话已关闭。	1
Echo 会话被拒绝	18359	指示 Echo 会话已遭拒绝。	3
Echo 会话正在进行中	18360	指示正在进行 Echo 会话。	1
远程 .NET 会话已打开	18361	指示远程 .NET 会话已建立。	1
远程 .NET 会话已关闭	18362	指示远程 .NET 会话已关闭。	1
远程 .NET 会话已重置	18363	指示远程 .NET 会话已重置。	3
远程 .NET 会话已终止	18364	指示远程 .NET 会话已终止。	3
远程 .NET 会话被拒绝	18365	指示远程 .NET 会话已遭拒绝。	3
远程 .NET 会话正在进行中	18366	指示正在进行远程 .NET 会话。	1
DNP3 会话已打开	18367	指示分布式网络协议 (DNP3) 会话已建立。	1
DNP3 会话已关闭	18368	指示 DNP3 会话已关闭。	1

表 57. 应用程序类别的低级类别和严重性级别 (续)

低级别事件类别	类别标识	描述	严重性级别 (0 - 10)
DNP3 会话已重置	18369	指示 DNP3 会话已重置。	3
DNP3 会话已终止	18370	指示 DNP3 会话已终止。	3
DNP3 会话被拒绝	18371	指示 DNP3 会话已遭拒绝。	3
DNP3 会话正在进行中	18372	指示正在进行 DNP3 会话。	1
Discard 会话已打开	18373	指示 Discard 会话已建立。	1
Discard 会话已关闭	18374	指示 Discard 会话已关闭。	1
Discard 会话已重置	18375	指示 Discard 会话已重置。	3
Discard 会话已终止	18376	指示 Discard 会话已终止。	3
Discard 会话被拒绝	18377	指示 Discard 会话已遭拒绝。	3
Discard 会话正在进行中	18378	指示正在进行 Discard 会话。	1
DHCP 会话已打开	18379	指示动态主机配置协议 (DHCP) 会话已建立。	1
DHCP 会话已关闭	18380	指示 DHCP 会话已关闭。	1
DHCP 会话被拒绝	18381	指示 DHCP 会话已遭拒绝。	3
DHCP 会话正在进行中	18382	指示正在进行 DHCP 会话。	1
DHCP 成功	18383	指示已成功获取 DHCP 租约	1
DHCP 失败	18384	指示无法获取 DHCP 租约	3
CVS 会话已打开	18385	指示并发版本控制系统 (CVS) 会话已建立。	1
CVS 会话已关闭	18386	指示 CVS 会话已关闭。	1
CVS 会话已重置	18387	指示 CVS 会话已重置。	3
CVS 会话已终止	18388	指示 CVS 会话已终止。	3
CVS 会话被拒绝	18389	指示 CVS 会话已遭拒绝。	3
CVS 会话正在进行中	18390	指示正在进行 CVS 会话。	1
CUPS 会话已打开	18391	指示通用 UNIX 打印系统 (CUPS) 会话已建立。	1
CUPS 会话已关闭	18392	指示 CUPS 会话已关闭。	1

表 57. 应用程序类别的低级类别和严重性级别 (续)

低级别事件类别	类别标识	描述	严重性级别 (0 - 10)
CUPS 会话已重置	18393	指示 CUPS 会话已重置。	3
CUPS 会话已终止	18394	指示 CUPS 会话已终止。	3
CUPS 会话被拒绝	18395	指示 CUPS 会话已遭拒绝。	3
CUPS 会话正在进行中	18396	指示正在进行 CUPS 会话。	1
Chargen 会话已开始	18397	指示字符生成器 (Chargen) 会话已开始。	1
Chargen 会话已关闭	18398	指示 Chargen 会话已关闭。	1
Chargen 会话已重置	18399	指示 Chargen 会话已重置。	3
Chargen 会话已终止	18400	指示 Chargen 会话已终止。	3
Chargen 会话被拒绝	18401	指示 Chargen 会话已遭拒绝。	3
Chargen 会话正在进行中	18402	指示正在进行 Chargen 会话。	1
其他 VPN	18403	指示已检测到其他 VPN 会话	1
DAP 会话已开始	18404	指示 DAP 会话已建立。	1
DAP 会话已结束	18405	指示 DAP 会话已结束。	1
DAP 会话被拒绝	18406	指示 DAP 会话已遭拒绝。	3
DAP 会话状态	18407	指示已发出 DAP 会话状态请求。	1
DAP 会话正在进行中	18408	指示正在进行 DAP 会话。	1
DAP 认证失败	18409	指示 DAP 认证失败。	4
DAP 认证成功	18410	指示 DAP 认证成功。	1
TOR 会话已开始	18411	指示 TOR 会话已建立。	1
TOR 会话已关闭	18412	指示 TOR 会话已关闭。	1
TOR 会话已重置	18413	指示 TOR 会话已重置。	3
TOR 会话已终止	18414	指示 TOR 会话已终止。	3
TOR 会话被拒绝	18415	指示 TOR 会话已遭拒绝。	3
TOR 会话正在进行中	18416	指示正在进行 TOR 会话。	1
Game 会话已开始	18417	指示 Game 会话已开始。	1

表 57. 应用程序类别的低级类别和严重性级别 (续)

低级别事件类别	类别标识	描述	严重性级别 (0 - 10)
Game 会话已关闭	18418	指示 Game 会话已关闭。	1
Game 会话已重置	18419	指示 Game 会话已重置。	3
Game 会话已终止	18420	指示 Game 会话已终止。	3
Game 会话被拒绝	18421	指示 Game 会话已遭拒绝。	3
Game 会话正在进行中	18422	指示正在进行 Game 会话。	1
管理员登录尝试	18423	指示已检测到使用管理用户身份进行登录的尝试。	2
用户登录尝试	18424	指示已检测到使用非管理用户身份进行登录的尝试。	2
客户机服务器	18425	指示客户机/服务器活动。	1
内容交付	18426	指示内容交付活动。	1
数据传输	18427	指示数据传输。	3
数据仓储	18428	指示数据仓储活动。	3
目录服务	18429	指示目录服务活动。	2
文件打印	18430	指示文件打印活动。	1
文件传输	18431	指示文件传输。	2
Game	18432	指示 Game 活动。	4
医疗保健	18433	指示医疗保健活动。	1
内部系统	18434	指示内部系统活动。	1
因特网协议	18435	指示因特网协议活动。	1
遗留	18436	指示遗留活动。	1
邮件	18437	指示邮件活动。	1
其他	18438	指示其他活动。	2
多媒体	18439	指示多媒体活动。	2
网络管理	18440	指示网络管理活动。	
P2P	18441	指示对等 (P2P) 活动。	4
远程访问	18442	指示远程访问活动。	3
路由协议	18443	指示路由协议活动。	1
安全协议	18444	指示安全协议活动。	2
流	18445	指示流活动。	2
不常见的协议	18446	指示不常见的协议活动。	3
VoIP	18447	指示 VoIP 活动。	1

表 57. 应用程序类别的低级类别和严重性级别 (续)			
低级别事件类别	**类别标识**	**描述**	**严重性级别 (0 - 10)**
Web	18448	指示 Web 活动。	1
ICMP	18449	指示 ICMP 活动	1

审计

审计类别包含与审计活动相关的事件，如电子邮件或 FTP 活动。

下表描述了审计类别的低级事件类别和关联的严重性级别。

表 58. 审计类别的低级类别和严重性级别			
低级别事件类别	**类别标识**	**描述**	**严重性级别 (0 - 10)**
常规审计事件	19001	指示常规审计事件已开始。	1
内置执行	19002	指示内置审计任务已在运行。	1
批量复制	19003	指示已检测到批量数据复制。	1
数据转储	19004	指示已检测到数据转储。	1
数据导入	19005	指示已检测到数据导入。	1
数据选择	19006	指示已检测到数据选择进程。	1
数据截断	19007	指示已检测到数据截断进程。	1
数据更新	19008	指示已检测到数据更新进程。	1
过程/触发器执行	19009	指示已检测到数据库过程或触发器的执行。	1
模式更改	19010	指示已更改过程或触发器的执行模式。	1
已尝试创建活动	19011	指示已尝试创建活动。	1
创建活动成功	19012	指示已成功创建活动。	1
创建活动失败	19013	指示创建活动失败。	3
已尝试读取活动	19014	指示已尝试读取活动。	1
读取活动成功	19015	指示已成功读取活动。	1
读取活动失败	19016	指示读取活动失败。	3
已尝试更新活动	19017	指示已尝试更新活动。	1
更新活动成功	19018	指示已成功更新活动。	1
更新活动失败	19019	指示更新活动失败。	3
已尝试删除活动	19020	指示已尝试删除活动。	1
删除活动成功	19021	指示已成功删除活动。	1

表 *58.* 审计类别的低级类别和严重性级别 *(续)*

低级别事件类别	**类别标识**	**描述**	**严重性级别 (0 - 10)**
删除活动失败	19022	指示删除活动失败。	3
已尝试备份活动	19023	指示已尝试备份活动。	1
备份活动成功	19024	指示已成功备份活动。	1
备份活动失败	19025	指示备份活动失败。	3
已尝试捕获活动	19026	指示已尝试捕获活动。	1
捕获活动成功	19027	指示已成功捕获活动。	1
捕获活动失败	19028	指示捕获活动失败。	3
已尝试配置活动	19029	指示已尝试配置活动。	1
配置活动成功	19030	指示已成功配置活动。	1
配置活动失败	19031	指示配置活动失败。	3
已尝试部署活动	19032	指示已尝试部署活动。	1
部署活动成功	19033	指示已成功部署活动。	1
部署活动失败	19034	指示部署活动失败。	3
已尝试禁用活动	19035	指示已尝试禁用活动。	1
禁用活动成功	19036	指示已成功禁用活动。	1
禁用活动失败	19037	指示禁用活动失败。	3
已尝试启用活动	19038	指示已尝试启用活动。	1
启用活动成功	19039	指示已成功启用活动。	1
启用活动失败	19040	指示启用活动失败。	3
已尝试监视活动	19041	指示已尝试监视活动。	1
监视活动成功	19042	指示已成功监视活动。	1
监视活动失败	19043	指示监视活动失败。	3
已尝试恢复活动	19044	指示已尝试恢复活动。	1
恢复活动成功	19045	指示已成功恢复活动。	1
恢复活动失败	19046	指示恢复活动失败。	3
已尝试开始活动	19047	指示已尝试开始活动。	1
开始活动成功	19048	指示已成功开始活动。	1
开始活动失败	19049	指示开始活动失败。	3
已尝试停止活动	19050	指示已尝试停止活动。	1
停止活动成功	19051	指示已成功停止活动。	1
停止活动失败	19052	指示停止活动失败。	3
已尝试取消部署活动	19053	指示已尝试取消部署活动。	1
取消部署活动成功	19054	指示已成功取消部署活动。	1

表 58. 审计类别的低级类别和严重性级别 (续)			
低级别事件类别	**类别标识**	**描述**	**严重性级别 (0 - 10)**
取消部署活动失败	19055	指示取消部署活动失败。	3
已尝试接收活动	19056	指示已尝试接收活动。	1
接收活动成功	19057	指示已成功接收活动。	1
接收活动失败	19058	指示接收活动失败。	3
已尝试发送活动	19059	指示已尝试发送活动。	1
发送活动成功	19060	指示已成功发送活动。	1
发送活动失败	19061	指示发送活动失败。	3

控制

控制类别包含硬件系统相关的事件。

下表描述了控制类别的低级事件类别和关联的严重性级别。

表 59. 控制类别的低级类别和严重性级别			
低级别事件类别	**类别标识**	**描述**	**严重性级别 (0 - 10)**
设备读取	22001	指示读取的设备。	1
设备通信	22002	指示与设备进行的通信。	1
设备审计	22003	指示发生设备审计。	1
设备事件	22004	指示发生设备事件。	1
设备 Ping	22005	指示对设备发生了 ping 操作。	1
设备配置	22006	指示已配置设备。	1
设备注册	22007	指示已注册设备。	1
设备路由	22008	指示发生的设备路由操作。	1
设备导入	22009	指示已发生设备导入。	1
设备信息	22010	指示已发生设备信息操作。	1
设备警告	22011	指示设备上已生成警告。	1
设备错误	22012	指示设备上生成了错误。	1
中继设备事件	22013	指示中继事件。	1
NIC 事件	22014	指示网络接口卡 (NIC) 事件。	1
UIQ 事件	22015	指示移动设备上发生的事件。	1
IMU 事件	22016	指示集成管理单元 (IMU) 上发生的事件。	1
记帐事件	22017	指示记帐事件。	1

表 59. 控制类别的低级类别和严重性级别 (续)			
低级别事件类别	**类别标识**	**描述**	**严重性级别 (0 - 10)**
DBMS 事件	22018	指示数据库管理系统 (DBMS) 上的事件。	1
导入事件	22019	指示已发生导入。	1
位置导入	22020	指示发生导入的位置。	1
路由导入	22021	指示已发生路由导入。	1
导出事件	22022	指示已发生导出。	1
远程信号	22023	指示发生远程信号。	1
网关状态	22024	指示网关状态。	1
作业事件	22025	指示已发生作业。	1
安全事件	22026	指示已发生安全性事件。	1
设备篡改检测	22027	指示系统检测到篡改操作。	1
时间事件	22028	指示已发生时间事件。	1
可疑行为	22029	指示已发生可疑行为。	1
电源中断	22030	指示已发生电源中断。	1
电源恢复	22031	指示电源已复原。	1
脉动信号	22032	指示已发生脉动信号 ping。	1
远程连接事件	22033	指示到系统的远程连接。	1

资产概要分析程序

资产概要分析程序类别包含与资产概要文件相关的事件。

下表描述了概要分析程序类别的低级事件类别和关联的严重性级别。

表 60. 概要分析程序类别的低级类别和严重性级别			
低级别事件类别	**类别标识**	**描述**	**严重性级别 (0 - 10)**
资产已创建	23001	指示已创建资产。	1
资产已更新	23002	指示已更新资产。	1
资产已观测	23003	指示已观测资产。	1
资产已移动	23004	指示已移动资产。	1
资产已删除	23005	指示已删除资产。	1
资产主机名已清除	23006	指示已清除主机名。	1
资产主机名已创建	23007	指示已创建主机名。	1
资产主机名已更新	23008	指示已更新主机名。	1
资产主机名已观测	23009	指示已观测主机名。	1
资产主机名已移动	23010	指示已移动主机名。	1

表 60. 概要分析程序类别的低级类别和严重性级别 (续)

低级别事件类别	类别标识	描述	严重性级别 (0 - 10)
资产主机名已删除	23011	指示已删除主机名。	1
资产端口已清除	23012	指示已清除端口。	1
资产端口已创建	23013	指示已创建端口。	1
资产端口已更新	23014	指示已更新端口。	1
资产端口已观测	23015	指示已观测端口。	1
资产端口已移动	23016	指示已移动端口。	1
资产端口已删除	23017	指示已删除端口。	1
资产漏洞实例已清除	23018	指示已清除漏洞实例。	1
资产漏洞实例已创建	23019	指示已创建漏洞实例。	1
资产漏洞实例已更新	23020	指示已更新漏洞实例。	1
资产漏洞实例已观测	23021	指示已观测漏洞实例。	1
资产漏洞实例已移动	23022	指示已移动漏洞实例。	1
资产漏洞实例已删除	23023	指示已删除漏洞实例。	1
资产操作系统已清除	23024	指示已清除操作系统。	1
资产操作系统已创建	23025	指示已创建操作系统。	1
资产操作系统已更新	23026	指示已更新操作系统。	1
资产操作系统已观测	23027	指示已观测操作系统。	1
资产操作系统已移动	23028	指示已移动操作系统。	1
资产操作系统已删除	23029	指示已删除操作系统。	1
资产属性已清除	23030	指示已清除属性。	1
资产属性已创建	23031	指示已创建属性。	1
资产属性已更新	23032	指示已更新属性。	1
资产属性已观测	23033	指示已观测属性。	1
资产属性已移动	23034	指示已移动属性。	1
资产属性已删除	23035	指示已移动属性。	1
资产 IP 地址已清除	23036	指示已清除 IP 地址。	1
资产 IP 地址已创建	23037	指示已创建 IP 地址。	1
资产 IP 地址已更新	23038	指示已更新 IP 地址。	1
资产 IP 地址已观测	23039	指示已观测 IP 地址。	1
资产 IP 地址已移动	23040	指示已移动 IP 地址。	1
资产 IP 地址已删除	23041	指示已删除 IP 地址。	1
资产接口已清除	23042	指示已清除接口。	1
资产接口已创建	23043	指示已创建接口。	1
资产接口已更新	23044	指示已更新接口。	1

表 60. 概要分析程序类别的低级类别和严重性级别 (续)

低级别事件类别	类别标识	描述	严重性级别 (0 - 10)
资产接口已观测	23045	指示已观测接口。	1
资产接口已移动	23046	指示已移动接口。	1
资产接口已合并	23047	指示已合并接口。	1
资产接口已删除	23048	指示已删除接口。	1
资产用户已清除	23049	指示已清除用户。	1
资产用户已观测	23050	指示已观测用户。	1
资产用户已移动	23051	指示已移动用户。	1
资产用户已删除	23052	指示已删除用户。	1
资产扫描策略已清除	23053	指示已清除扫描策略。	1
资产扫描策略已观测	23054	指示已观测扫描策略。	1
资产扫描策略已移动	23055	指示已移动扫描策略。	1
资产扫描策略已删除	23056	指示已删除扫描策略。	1
资产 Windows 应用程序已清除	23057	指示已清除 Windows 应用程序。	1
资产 Windows 应用程序已观测	23058	指示已观测 Windows 应用程序。	1
资产 Windows 应用程序已移动	23059	指示已移动 Windows 应用程序。	1
资产 Windows 应用程序已删除	23060	指示已删除 Windows 应用程序。	1
资产扫描服务已清除	23061	指示已清除扫描服务。	1
资产扫描服务已观测	23062	指示已观测扫描服务。	1
资产扫描服务已移动	23063	指示已移动扫描服务。	1
资产扫描服务已删除	23064	指示已删除扫描服务。	1
资产 Windows 补丁已清除	23065	指示已清除 Windows 补丁。	1
资产 Windows 补丁已观测	23066	指示已观测 Windows 补丁。	1
资产 Windows 补丁已移动	23067	指示已移动 Windows 补丁。	1
资产 Windows 补丁已删除	23068	指示已删除 Windows 补丁。	1
资产 UNIX 补丁已清除	23069	指示已清除 UNIX 补丁。	1
资产 UNIX 补丁已观测	23070	指示已观测 UNIX 补丁。	1
资产 UNIX 补丁已移动	23071	指示已移动 UNIX 补丁。	1
资产 UNIX 补丁已删除	23072	指示已删除 UNIX 补丁。	1
资产补丁扫描已清除	23073	指示已清除补丁扫描。	1

表 60. 概要分析程序类别的低级类别和严重性级别 (续)			
低级别事件类别	**类别标识**	**描述**	**严重性级别 (0 - 10)**
资产补丁扫描已创建	23074	指示已创建补丁扫描。	1
资产补丁扫描已移动	23075	指示已移动补丁扫描。	1
资产补丁扫描已删除	23076	指示已删除补丁扫描。	1
资产端口扫描已清除	23077	指示已清除端口扫描。	1
资产端口扫描已创建	23078	指示已清除端口扫描。	1
资产端口扫描已移动	23079	指示已移动补丁扫描。	1
资产端口扫描已删除	23080	指示已删除补丁扫描。	1
资产客户机应用程序已清除	23081	指示已清除客户机应用程序。	1
资产客户机应用程序已观测	23082	指示已观测客户机应用程序。	1
资产客户机应用程序已移动	23083	指示已移动客户机应用程序。	1
资产客户机应用程序已删除	23084	指示已删除客户机应用程序。	1
资产补丁扫描已观测	23085	指示已观测补丁扫描。	1
资产端口扫描已观测	23086	指示已观测端口扫描。	1
NetBIOS 组已创建	23087	指示已创建 NetBIOS 组。	1
NetBIOS 组已更新	23088	指示已更新 NetBIOS 组。	1
NetBIOS 组已观测	23089	指示已观测 NetBIOS 组。	1
NetBIOS 组已删除	23090	指示已删除 NetBIOS 组。	1
NetBIOS 组已清除	23091	指示已清除 NetBIOS 组。	1
NetBIOS 组已移动	23092	指示已移动 NetBIOS 组。	1

感应

感应类别包含与感应用户行为分析相关的事件。

下表描述感应类别的低级别事件类别和关联的严重性级别。

表 61.			
低级别事件类别	**类别标识**	**描述**	**严重性级别 (0 - 10)**
用户行为	24001	指示用户的行为。	5
用户布局	24002	指示用户的地理位置。	5

表 61. (续)

低级别事件类别	类别标识	描述	严重性级别 (0 - 10)
用户时间	24003	指示用户的时间。	5
用户访问权	24004	指示用户的访问权。	5
用户特权	24005	指示用户的特权。	5
用户风险	24006	指示用户的风险。	5
意识攻击	24007	指示发生感应攻击。	5
资源风险	24008	指示存在风险的资源。	5

第 21 章 QRadar 使用的公共端口和服务器

IBM QRadar 需要特定端口准备好接收来自 QRadar 组件和外部基础结构的信息。要确保 QRadar 正在使用最新安全信息，还需要访问公共服务器和 RSS 订阅源。

端口 22 上的 SSH 通信

QRadar 控制台用于与受管主机通信的所有端口可通过 SSH 在端口 22 上创建加密隧道。

控制台使用加密的 SSH 会话连接到受管主机以进行安全通信。从控制台启动这些 SSH 会话以向受管主机提供数据。例如，QRadar Console 可启动到 事件处理器 设备的多个 SSH 会话以进行安全通信。此通信可包含通过 SSH 的隧道端口，例如，针对端口 443 的 HTTPS 数据和针对端口 32006 的 Ariel 查询数据。使用加密的 IBM QRadar QFlow Collector 可启动到查询数据的流处理器设备的 SSH 会话。

QRadar 不需要的开放端口

在以下情况下，您可能会查找其他开放端口：

- 在自己的硬件上安装 QRadar 时，您可能看到 Red Hat Enterprise Linux 中包含的服务、守护程序和程序使用的开放端口。
- 在安装或导出网络文件共享时，您可能看到 RPC 服务需要的动态分配的端口，例如，`rpc.mountd` 和 `rpc.rquotad`。

相关概念

IBM QRadar 产品中的功能

QRadar 端口使用情况

复查 IBM QRadar 服务和组件用于在网络中进行通信的公共端口列表。您可使用端口列表来确定网络中必须打开的端口。例如，可确定必须打开哪些端口才能使 QRadar Console 与远程事件处理器进行通信。

WinCollect 远程轮询

远程轮询其他 Microsoft Windows 操作系统的 WinCollect 代理程序可能需要分配其他端口。

有关更多信息，请参阅《IBM QRadar WinCollect 用户指南》。

QRadar 侦听端口

下表显示了已打开并处于 `LISTEN` 状态的 QRadar 端口。仅当系统上已启用 iptables 时，`LISTEN` 端口才有效。除非另有说明，否则有关已分配的端口号的信息适用于所有 QRadar 产品。

表 62. 供 *QRadar* 服务和组件使用的侦听端口

端口	描述	协议	方向	要求
22	SSH	TCP	从 QRadar Console 到所有其他组件之间的双向流量。	远程管理访问。 添加远程系统作为受管主机。 从外部设备检索文件的日志源协议，例如，日志文件协议。 使用命令行界面从桌面与 Console 进行通信的用户。 高可用性 (HA)。
25	SMTP	TCP	从所有受管主机到 SMTP 网关。	从 QRadar 到 SMTP 网关的电子邮件。 向电子邮件管理联系人交付错误和警告电子邮件消息。

表 62. 供 *QRadar* 服务和组件使用的侦听端口 *(续)*

端口	描述	协议	方向	要求
111	端口映射器	TCP/UDP	与 QRadar Console 通信的受管主机。 连接到 QRadar Console 的用户。	所需服务的远程过程调用 (RPC)，例如，网络文件系统 (NFS)。
123	网络时间协议 (NTP)	TCP/UDP	QRadar Console 到 NTP 服务器。 HA 主要主机到辅助主机，反之亦然	QRadar HA 对之间的时间同步以及 QRadar Console 与 NTP 服务器之间的时间同步。
135 和用于 RPC 调用的动态分配的端口（高于 1024）。	DCOM	TCP	WinCollect 代理程序与远程轮询其中事件的 Windows 操作系统之间的双向流量。 使用 Microsoft 安全性事件日志协议或自适应日志导出器代理程序的 QRadar Console 组件或 IBM QRadar 事件收集器与远程轮询其中事件的 Windows 操作系统之间的双向流量。	此流量是由 WinCollect、Microsoft 安全性事件日志协议或自适应日志导出器生成的。 **注:** DCOM 通常会为通信分配随机端口范围。您可以将 Microsoft Windows 产品配置为使用特定端口。有关更多信息，请参阅 Microsoft Windows 文档。
137	Windows NetBIOS 名称服务	UDP	WinCollect 代理程序与远程轮询其中事件的 Windows 操作系统之间的双向流量。 使用 Microsoft 安全性事件日志协议或自适应日志导出器代理程序的 QRadar Console 组件或 QRadar Event Collector 与远程轮询其中事件的 Windows 操作系统之间的双向流量。	此流量是由 WinCollect、Microsoft 安全性事件日志协议或自适应日志导出器生成的。
138	Windows NetBIOS 数据报服务	UDP	WinCollect 代理程序与远程轮询其中事件的 Windows 操作系统之间的双向流量。 使用 Microsoft 安全性事件日志协议或自适应日志导出器代理程序的 QRadar Console 组件或 QRadar Event Collector 与远程轮询其中事件的 Windows 操作系统之间的双向流量。	此流量是由 WinCollect、Microsoft 安全性事件日志协议或自适应日志导出器生成的。
139	Windows NetBIOS 会话服务	TCP	WinCollect 代理程序与远程轮询其中事件的 Windows 操作系统之间的双向流量。 使用 Microsoft 安全性事件日志协议或自适应日志导出器代理程序的 QRadar Console 组件或 QRadar Event Collector 与远程轮询其中事件的 Windows 操作系统之间的双向流量。	此流量是由 WinCollect、Microsoft 安全性事件日志协议或自适应日志导出器生成的。
162	NetSNMP	UDP	连接到 QRadar Console 的 QRadar 受管主机。 外部日志源到 QRadar Event Collector。	用于侦听来自外部日志源的通信（v1、v2c 和 v3）的 NetSNMP 守护程序的 UDP 端口。仅当启用 SNMP 代理时，此端口才会打开。
199	NetSNMP	TCP	连接到 QRadar Console 的 QRadar 受管主机。 外部日志源到 QRadar Event Collector。	用于侦听来自外部日志源的通信（v1、v2c 和 v3）的 NetSNMP 守护程序的 TCP 端口。仅当启用 SNMP 代理时，此端口才会打开。
427	服务位置协议 (SLP)	UDP/TCP		集成管理模块使用此端口来查找 LAN 上的服务。

表 62. 供 *QRadar* 服务和组件使用的侦听端口 *(续)*

端口	描述	协议	方向	要求
443	Apache/HTTPS	TCP	从所有产品到 QRadar Console 的安全通信的双向流量。	配置从 QRadar Console 到受管主机的下载。 连接到 QRadar Console 的 QRadar 受管主机。 用户必须登录才能访问 QRadar。 为 WinCollect 代理程序管理并提供配置更新的 QRadar Console。
445	Microsoft 目录服务	TCP	WinCollect 代理程序与远程轮询其中事件的 Windows 操作系统之间的双向流量。 使用 Microsoft 安全性事件日志协议的 QRadar Console 组件或 QRadar Event Collector 与远程轮询其中事件的 Windows 操作系统之间的双向流量。 自适应日志导出器代理程序与远程轮询其中事件的 Windows 操作系统之间的双向流量。	此流量是由 WinCollect、Microsoft 安全性事件日志协议或自适应日志导出器生成的。
514	Syslog	UDP/TCP	提供 TCP syslog 事件的外部网络设备使用双向流量。 提供 UDP syslog 事件的外部网络设备使用单向流量。 从 QRadar 主机到 QRadar Console 的内部 syslog 流量。	向 QRadar 组件发送事件数据的外部日志源。 Syslog 流量包括 WinCollect 代理程序、事件收集器和自适应日志导出器代理程序能够向 QRadar 发送 UDP 或 TCP 事件。
762	网络文件系统 (NFS) 安装守护程序 (mountd)	TCP/UDP	QRadar Console 与 NFS 服务器之间的连接。	网络文件系统 (NFS) 安装守护程序，用于处理在指定位置安装文件系统的请求。
1514	Syslog-ng	TCP/UDP	本地 事件收集器 组件和本地事件处理器组件之间的连接，连接到 syslog-ng 守护程序以进行日志记录。	用于 syslog-ng 的内部日志记录端口。
2049	NFS	TCP	QRadar Console 与 NFS 服务器之间的连接。	用于在组件之间共享文件或数据的网络文件系统 (NFS) 协议。
2055	NetFlow 数据	UDP	从流源（通常为路由器）上的管理接口到 IBM QRadar QFlow Collector。	来自组件（例如，路由器）的 NetFlow 数据报。
2375	Docker 命令端口	TCP	内部通信。此端口在外部不可用。	用于管理 QRadar 应用程序框架资源。
3389	基于 USB 的远程桌面协议 (RDP) 和以太网已启用	TCP/UDP		如果 Microsoft Windows 操作系统配置为基于 USB 的 RDP 和以太网，那么用户可以通过管理网络启动到服务器的会话。这意味着 RDP 的缺省端口 3389 必须处于打开状态。
3900	集成管理模块远程存在端口	TCP/UDP		该端口用于通过集成管理模块与 QRadar Console 进行交互。
4333	重定向端口	TCP		此端口在 QRadar 攻击解析中被指定为地址解析协议 (ARP) 请求的重定向端口。

表 62. 供 *QRadar* 服务和组件使用的侦听端口 *(续)*

端口	描述	协议	方向	要求
5000	用于允许与 Console 上运行的 docker si-registry 进行通信。它允许所有受管主机从 Console 提取将用于创建本地容器的映像。	TCP	从 QRadar 受管主机到 QRadar Console 的单向流量。该端口仅在 Console 上处于打开状态。受管主机必须从 Console 提取。	它对于应用程序主机上运行的应用程序是必需的。
5432	Postgres	TCP	供用于访问本地数据库实例的受管主机用于通信。	它是从**管理**选项卡配置受管主机所必需的。
6514	Syslog	TCP	提供加密 TCP syslog 事件的外部网络设备使用双向流量。	向 QRadar 组件发送加密事件数据的外部日志源。
7676、7677 和高于 32000 的四个随机绑定端口。	消息传递连接 (IMQ)	TCP	受管主机上的组件之间的消息队列通信。	用于受管主机上的组件之间的通信的消息队列代理程序。 **注:** 您必须允许从 QRadar Console 上的这些端口到未加密的主机的访问。 端口 7676 和 7677 为静态 TCP 端口，在随机端口上创建四个额外连接。
7777、7778、7779、7780、7781、7782、7783、7788、7790、7791、7792、7793、7795、7799 和 8989。	JMX 服务器端口	TCP	内部通信。这些端口在外部不可用。	JMX 服务器（Java 管理 Bean）监视所有内部 QRadar 进程以公开可支持性度量。 这些端口由 QRadar 支持团队管理。
7789	HA 分布式复制块设备	TCP/UDP	在 HA 集群中的辅助主机与主要主机之间的双向流量。	分布式复制块设备用于保持 HA 配置中的主要主机与辅助主机之间的驱动器同步。
7800	Apache Tomcat	TCP	从 事件处理器 到 QRadar Console。	针对事件实时进行操作（流）。
7801	Apache Tomcat	TCP	从 事件处理器 到 QRadar Console。	针对流实时进行操作（流）。
7803	异常检测引擎	TCP	从 事件处理器 到 QRadar Console。	异常检测引擎端口。
7804	QRM ARC 构建器	TCP	QRadar 进程与 ARC 构建器之间的内部控制通信。	此端口仅用于 QRadar Risk Manager。在外部不可用。
8000	事件收集服务 (ECS)	TCP	从 事件收集器 到 QRadar Console。	特定事件收集服务 (ECS) 的侦听端口。
8001	SNMP 守护程序端口	TCP	从 QRadar Console 请求 SNMP 陷阱信息的外部 SNMP 系统。	外部 SNMP 数据请求的侦听端口。
8005	Apache Tomcat	TCP	内部通信。在外部不可用。	打开以控制 tomcat。 此端口为绑定端口，仅接受来自本地主机的连接。
8009	Apache Tomcat	TCP	从 HTTP 守护程序 (HTTPd) 进程到 Tomcat	Tomcat 接口，用于使用并通过代理连接请求以用于 Web Service。
8080	Apache Tomcat	TCP	从 HTTP 守护程序 (HTTPd) 进程到 Tomcat	Tomcat 接口，用于使用并通过代理连接请求以用于 Web Service。

表 62. 供 *QRadar* 服务和组件使用的侦听端口 *(续)*

端口	描述	协议	方向	要求
8082	QRadar Risk Manager 的安全通道	TCP	QRadar Console 和 QRadar Risk Manager 之间的双向流量	在 QRadar Risk Manager 和 QRadar Console 之间使用加密时必需。
8413	WinCollect 代理程序	TCP	WinCollect 代理程序与 QRadar Console 之间的双向流量。	此流量是由 WinCollect 代理程序生成的，并且通信已加密。它是向 WinCollect 代理程序提供配置更新和以已连接方式使用 WinCollect 所必需的。
8844	Apache Tomcat	TCP	从 QRadar Console 到运行 QRadar Vulnerability Manager 处理器的设备的单向流量。	供 Apache Tomcat 用于从运行 QRadar Vulnerability Manager 处理器的主机读取 RSS 订阅源。
9000	Conman	TCP	从 QRadar Console 到 QRadar 应用程序主机的单向流量。	与应用程序主机配合使用。允许控制台将应用程序部署到应用程序主机和管理这些应用程序。
9090	XForce IP 声誉数据库和服务器	TCP	内部通信。在外部不可用。	QRadar 进程与 XForce 声誉 IP 数据库之间的通信。
9381	证书文件下载	TCP	从 QRadar 受管主机或外部网络到 QRadar Console 的单向流量	下载 QRadar CA 证书和 CRL 文件，这些文件可用于验证 QRadar 生成的证书。
9913 加上一个动态分配的端口	Web 应用程序容器	TCP	Java 虚拟机之间的双向 Java 远程方法调用 (RMI) 通信	注册 Web 应用程序时，会动态分配一个额外端口。
9995	NetFlow 数据	UDP	从流源（通常为路由器）上的管理接口到 QRadar QFlow Collector。	来自组件（例如，路由器）的 NetFlow 数据报。
9999	IBM QRadar Vulnerability Manager 处理器	TCP	从扫描程序到运行 QRadar Vulnerability Manager 处理器的设备的单向流量	用于 QRadar Vulnerability Manager (QVM) 命令信息。QRadar Console 连接到运行 QRadar Vulnerability Manager 处理器的主机上的该端口。仅当启用 QVM 时，才可使用此端口。
10000	QRadar 基于 Web 的系统管理接口	TCP/UDP	用户桌面系统到所有 QRadar 主机。	在 QRadar V7.2.5 和更低版本中，此端口用于服务器更改，例如，主机 root 用户密码和防火墙访问。 在 V7.2.6 中禁用端口 10000。
10101 和 10102	脉动信号命令	TCP	主 HA 节点和辅助 HA 节点之间的双向流量。	这是确保 HA 节点仍处于活动状态所必需的。
15433	Postgres	TCP	供用于访问本地数据库实例的受管主机用于通信。	用于 QRadar Vulnerability Manager (QVM) 配置和存储。仅当启用 QVM 时，才可使用此端口。
20000-23000	SSH 隧道	TCP	从 QRadar Console 到所有其他已加密的受管主机的双向流量。	SSH 隧道的本地侦听点，这些 SSH 隧道用于 Java 消息服务 (JMS) 与已加密的受管主机之间的通信。用于执行长期运行的异步任务，例如，通过“系统和许可证管理”来更新网络配置。
23111	SOAP Web 服务器	TCP		用于事件收集服务 (ECS) 的 SOAP Web 服务器端口。

表 62. 供 *QRadar* 服务和组件使用的侦听端口 *(续)*

端口	描述	协议	方向	要求
23333	Emulex 光纤通道	TCP	通过光纤通道卡连接到 QRadar 设备的用户桌面系统。	Emulex 光纤通道 HBAnywhere 远程管理服务 (elxmgmt)。
32000	规范化流转发	TCP	QRadar 组件之间的双向通信。	从非现场来源或在 QRadar QFlow Collector 之间传递的规范化流数据。
32004	规范化事件转发	TCP	QRadar 组件之间的双向通信。	非现场来源或 QRadar Event Collector 之间传递的规范化事件数据。
32005	数据流	TCP	QRadar 组件之间的双向通信。	单独的受管主机上的 QRadar Event Collector 之间的数据流通信端口。
32006	Ariel 查询	TCP	QRadar 组件之间的双向通信。	Ariel 代理服务器与 Ariel 查询服务器之间的通信端口。
32007	攻击数据	TCP	QRadar 组件之间的双向通信。	影响攻击或参与全局关联的事件和流。
32009	身份数据	TCP	QRadar 组件之间的双向通信。	被动漏洞信息服务 (VIS) 与事件收集服务 (ECS) 之间通信的身份数据。
32010	流侦听源端口	TCP	QRadar 组件之间的双向通信。	用于从 QRadar QFlow Collector 收集数据的流侦听端口。
32011	Ariel 侦听端口	TCP	QRadar 组件之间的双向通信。	Ariel 侦听端口，用于数据库搜索、进度信息和其他关联命令。
32000-33999	数据流（流、事件、流上下文）	TCP	QRadar 组件之间的双向通信。	数据流，例如，事件、流、流上下文和事件搜索查询。
40799	PCAP 数据	UDP	从 Juniper Networks SRX 系列设备到 QRadar。	从 Juniper Networks SRX 系列设备收集传入包捕获 (PCAP) 数据。 **注:** 设备上的包捕获可使用其他端口。有关配置包捕获的更多信息，请参阅 Juniper Networks SRX 系列设备文档。
ICMP	ICMP		在 HA 集群中的辅助主机与主要主机之间的双向流量。	使用因特网控制报文协议 (ICMP) 测试 HA 集群中的辅助主机与主要主机之间的网络连接。

QRadar 公共服务器

为了向您提供最新的安全信息，IBM QRadar 需要访问多个公共服务器和 RSS 订阅源。

公共服务器

表 63. *QRadar* 必须访问的公共服务器. 下表列出 QRadar 访问的 IP 地址或主机名的描述。

IP 地址或主机名	描述
194.153.113.31	IBM QRadar Vulnerability Manager DMZ 扫描程序
194.153.113.32	QRadar Vulnerability Manager DMZ 扫描程序

表 *63. QRadar* 必须访问的公共服务器. 下表列出 QRadar 访问的 IP 地址或主机名的描述。 *(续)*	
IP 地址或主机名	**描述**
qmmunity.q1labs.com	QRadar 自动更新服务器。 有关自动更新服务器的更多信息，请参阅 www.ibm.com/support (http://www-01.ibm.com/support/docview.wss?uid=swg21958881)。
qmmunity-eu.q1labs.com	QRadar 自动更新服务器。 有关自动更新服务器的更多信息，请参阅 www.ibm.com/support (http://www-01.ibm.com/support/docview.wss?uid=swg21958881)。
update.xforce-security.com	X-Force 威胁订阅源更新服务器
license.xforce-security.com	X-Force 威胁订阅源许可服务器

QRadar 产品的 RSS 订阅源

表 *64. RSS* 订阅源. 下表描述 QRadar 使用的 RSS 订阅源的需求。将 URL 复制到文本编辑器中并移除分页符，然后再粘贴到浏览器中。		
职务：	**URL**	**要求**
安全情报	http://feeds.feedburner.com/SecurityIntelligence	QRadar 和因特网连接
安全情报漏洞/威胁	http://securityintelligence.com/topics/vulnerabilities-threats/feed	QRadar 和因特网连接
IBM 我的通知	http://www-945.events.ibm.com/systems/support/myfeed/xmlfeeder.wss?feeder.requid= feeder.create_feed&feeder.feedtype=RSS&feeder.uid=270006EH0R&feeder.subscrid= S14b5f284d32&feeder.subdefkey=swgother&feeder.maxfeed=25	QRadar 和因特网连接
安全新闻	http://*IP_address_of_QVM_processor* :8844/rss/research/news.rss	已部署 IBM QRadar Vulnerability Manager 处理器
安全公告	http://*IP_address_of_QVM_processor* :8844/rss/research/advisories.rss	已部署 QRadar Vulnerability Manager 处理器
最新发布的漏洞	http://*IP_address_of_QVM_processor* :8844/rss/research/vulnerabilities.rss	已部署 QRadar Vulnerability Manager 处理器
扫描已完成	http://*IP_address_of_QVM_processor* :8844/rss/scanresults/completedScans.rss	已部署 QRadar Vulnerability Manager 处理器
扫描进行中	http://*IP_address_of_QVM_processor* :8844/rss/scanresults/runningScans.rss	已部署 QRadar Vulnerability Manager 处理器

第 22 章 RESTful API

当要将 IBM QRadar 与其他解决方案集成时，具象状态传输 (REST) 应用程序编程接口 (API) 很有用。您可以通过将 HTTPS 请求发送到 QRadar Console 上的特定端点 (URL)，来执行 QRadar Console 上的操作。

每个端点都包含要访问的资源的 URL 以及要在该资源上完成的操作。该操作由请求的 HTTP 方法表示：GET、POST、PUT 或 DELETE。有关每个端点的参数和响应的更多信息，请参阅 *IBM QRadar API Guide*。

QRadar API 论坛和代码样本

API 论坛提供有关 REST API 的更多信息，包括常见问题的答案和可在测试环境中使用的带注释代码样本。有关更多信息，请参阅 API 论坛 (https://ibm.biz/qradarforums)。

访问交互式 API 文档页面

使用交互式 API 文档页面来访问 RESTful API 的技术详细信息并试验向服务器发出 API 请求。

关于此任务

API 文档用户接口提供描述以及使用以下 REST API 接口的能力：

表 *65. REST API* 接口

REST API	**描述**
/api/analytics	创建、更新和移除规则的定制操作。
/api/ariel	查看事件和流属性，创建事件和流搜索以及管理搜索。
/api/asset_model	返回模型中所有资产的列表。您还可以列出所有可用资产属性类型和已保存搜索，以及更新资产。
/api/auth	注销当前会话并使其失效。
/api/config	查看和管理租户、域以及 QRadar 扩展。
/api/data_classification	查看所有高级别和低级别类别、QRadar 标识 (QID) 记录以及事件映射。您还可以创建或编辑 QID 记录和映射。
/api/forensics	管理捕获恢复和案例。
/api/gui_app_framework	安装和管理通过使用 GUI 应用程序框架软件开发套件创建的应用程序。
/api/help	返回 API 功能列表。
/api/qrm	管理 QRM 保存的搜索组、问题组、模拟组、拓扑保存的搜索组以及模型组。
/api/qvm	检索资产、漏洞、网络、开放式服务、网络和过滤器。您还可以创建或更新修复凭单。
/api/reference_data	查看和管理参考数据集合。
/api/scanner	查看、创建或启动与扫描概要文件相关的远程扫描。
/api/services	执行 WHOIS 查找、端口扫描查找、DNS 查找和 DIG 查找之类的任务。您还可以检索 IP 或 IP 集的地理位置数据。

表 *65. REST API* 接口 *(续)*	
REST API	**描述**
/api/siem	查看、更新和关闭攻击。您还可以添加注释和管理攻击关闭原因。
/api/staged_config	检索用户、主机、通知、远程网络和远程服务的暂存配置。您还可以启动或查看部署操作的状态，以及查看和删除 Yara 规则。
/api/system	管理服务器主机、网络接口和防火墙规则。

过程

1. 要访问交互式 API 文档接口，请在 Web 浏览器中输入以下 URL：`https://ConsoleIPaddress/api_doc/`。
2. 单击要使用的 API 版本旁边的箭头图标。
3. 转至要访问的端点。
4. 阅读端点文档并完成请求参数。
5. 单击**试验**以向控制台发送 API 请求并接收正确格式化的 HTTPS 响应。

   注: 单击**试验**时，将在 QRadar 系统上执行该操作。并非所有操作都可以撤销，例如，关闭攻击后无法将其重新打开。
6. 复审并收集与 QRadar 集成所需的信息。

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。

Linux 是 Linus Torvalds 在美国和/或其他国家或地区的注册商标。

UNIX 是 The Open Group 在美国和其他国家或地区的注册商标。

Java 和所有基于 Java 的商标和徽标是 Oracle 和/或其子公司的商标或注册商标。

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)。

通用数据保护条例

客户有责任确保自身遵守各种法律和法规，包括《欧盟通用数据保护条例》。客户须自行负责从合格的法律顾问那里，就可能会影响客户业务和客户为了遵守此类法律和法规需要采取的任何行动，获得关于任何相关法律和法规的认定和解释的意见。本文描述的产品、服务和其他功能不适用于所有客户情况，可能具有受限可用性。IBM 不提供法律、会计或审计意见，也不陈述或保证其服务或产品将确保客户遵守任何法律或法规。

要了解关于 IBM GDPR 就绪历程以及 GDPR 功能和服务的更多信息，请访问此处：https://ibm.com/gdpr

词汇表

本词汇表提供 IBM QRadar SIEM 软件及产品的术语和定义。

在本词汇表中，使用了下列交叉引用：

· 参见从非首选术语引用首选术语，或者从缩写引用完整形式。

· 另见引导您参考相关的或者对立的术语。

要了解其他术语和定义，请参阅 IBM Terminology Web 站点（在新窗口中打开）。

(B)

报告 (report)
在查询管理中，这是运行查询并对其应用某种格式而生成的格式化数据。

报告时间间隔 (report interval)
这是一个可配置的时间间隔，在此时间间隔结束时，事件处理器必须将捕获到的所有事件和流数据发送到控制台。

备用系统 (standby system)
这是在活动系统发生故障时自动进入活动状态的系统。如果启用了磁盘复制，那么此系统将从活动系统复制数据。

标准网络名称 (fully qualified network name, FQNN)
在网络层次结构中，这是包含所有部门的对象名称。下面是标准网络名称的一个示例：CompanyA.Department.Marketing。

标准域名 (fully qualified domain name, FQDN)
在因特网通信领域，这是主机系统的名称，其中包含域名的所有子名称。下面是标准域名的一个示例：rchland.vnet.ibm.com。

(C)

超流 (superflow)
这是由多个具有类似属性的流组成的单个流，旨在通过减少存储约束来增加处理能力。

重复流 (duplicate flow)
这是从不同流源接收到的同一数据传输的多个实例。

传输控制协议 (Transmission Control Protocol, TCP)
这是在因特网以及任何符合因特网工程任务组织 (IETF) 互联网络协议标准的网络中使用的通信协议。TCP 在包交换通信网络以及这类网络的互连系统中提供了可靠的主机到主机协议。另见因特网协议 (Internet Protocol)。

从本地到本地 (Local To Local, L2L)
与一个本地网络到另一本地网络的内部流量相关。

从本地到远程 (Local To Remote, L2R)
与一个本地网络到另一远程网络的内部流量相关。

从远程到本地 (Remote To Local, R2L)
这是从远程网络到本地网络的外部流量。

从远程到远程 (Remote To Remote, R2R)
这是从远程网络到另一远程网络的外部流量。

(D)

地址解析协议 (Address Resolution Protocol, ARP)
这是一种协议，用于将 IP 地址动态映射到局域网中的网络适配器地址。

动态主机配置协议 (Dynamic Host Configuration Protocol, DHCP)
这是一种通信协议，用于集中管理配置信息。例如，DHCP 向网络中的计算机自动分配 IP 地址。

端点 (endpoint)
环境中的 API 或服务的地址。API 显示一个端点并同时调用其他服务的端点。

(F)

非现场目标 (offsite target)
这是远离主站点的设备，用于接收来自事件收集器的事件或数据流。

非现场源 (offsite source)
这是远离主站点的设备，用于将规范化数据转发到事件收集器。

辅助 HA 主机 (secondary HA host)
这是连接到 HA 集群的备用计算机。主要 HA 主机发生故障时，辅助 HA 主机将承担主要 HA 主机的职责。

(G)

高可用性 (high availability, HA)
指发生节点或守护程序故障时重新配置集群系统，以便将工作负载重新分配到集群中的其余节点。

攻击 (offense)
这是作为对受监视条件的响应而发送的消息或生成的事件。例如，攻击将提供有关是否违反了某个策略或网络是否遭受攻击的信息。

管理共享 (administrative share)
对没有管理特权的用户隐藏的网络资源。管理共享为管理员提供对网络系统上的所有资源的访问权。

规模 (magnitude)
这是对特定攻击的相对重要性的度量。规模是根据相关性、严重性和可信性计算而得的加权值。

规则 (rule)
这是一组条件语句，这些语句使计算机系统能够识别关系并相应地运行自动化响应。

(H)

活动系统 (active system)
在高可用性 (HA) 集群中，这是其所有服务都处于运行状态的系统。

(J)

基于散列的消息认证代码 (Hash-Based Message Authentication Code, HMAC)
这是一种加密代码，它使用加密散列函数和密钥。

集合的引用映射 (reference map of sets)
这是将一个键映射到多个值的数据记录。例如，将特权用户列表映射到一个主机。

集群虚拟 IP 地址 (cluster virtual IP address)
这是在主要主机或辅助主机与 HA 集群之间共享的 IP 地址。

加密 (encryption)
在计算机安全性领域，这是将数据变换为某种难以理解的格式的过程，此过程使得原始数据不可获取或者只能通过解密过程获取。

简单网络管理协议 (Simple Network Management Protocol, SNMP)
这是一组协议，用于监视复杂网络中的系统和设备。有关受管设备的信息在管理信息库 (MIB) 中进行定义和存储。

结合时间间隔 (coalescing interval)
这是对事件进行捆绑的时间间隔。事件捆绑每 10 秒发生一次，并从第一个与当前结合的任何事件都不匹配的事件开始。在结合时间间隔内，前三个匹配事件将进行捆绑并发送到事件处理器。

解析顺序 (parsing order)
这是日志源定义，用户可以在其中定义共享同一个 IP 地址或主机名的日志源的重要性顺序。

局域网 (local area network, LAN)
这是一种网络，用于连接有限区域（例如单一建筑物或校园）中的多个设备，并且可以连接到更大型的网络。

(K)

开放式系统互连 (open systems interconnection, OSI)
这是符合国际标准化组织 (ISO) 信息交换标准的开放式系统互连。

开放式源代码漏洞数据库 (Open Source Vulnerability Database, OSVDB)
这是网络安全社区为网络安全社区创建的开放式源代码数据库，用于提供有关网络安全漏洞的技术信息。

可信性 (credibility)
这是介于 0 与 10 之间的数字评级，用于确定事件或攻击的完整性。随着多个源报告同一事件或攻击，可信性将增加。

客户机 (client)
这是一个软件程序或计算机，用于请求服务器提供服务。

控制台 (console)
这是一个显示站，操作员可以从中控制并观察系统操作。

(L)

累加器 (accumulator)
这是一个寄存器，可以在其中存储运算的其中一个操作数，该操作数随后将被该运算的结果替换。

流 (flow)
这是对话期间通过链路传递的单一数据传输。

流日志 (flow log)
这是流记录集合。

流源 (flow sources)
这是所捕获的流的来源。如果流来自受管主机上安装的硬件，那么将归类为内部流；如果流将发送到流收集器，那么将归类为外部流。

漏洞 (vulnerability)
操作系统、系统软件或应用程序软件组件中的安全隐患。

路由规则 (routing rule)
这是一个条件，事件数据满足此条件时，将执行条件收集和结果路由。

(M)

脉冲串 (burst)
传入事件或流的速度激增，导致超出许可的流或事件速度限制。

密钥文件 (key file)
在计算机安全性中，包含公用密钥、专用密钥、可信根和证书的文件。

(P)

凭证 (credential)
这是一组信息，用于将特定的访问权授予用户或进程。

(Q)

轻量级目录访问协议 (Lightweight Directory Access Protocol, LDAP)
这是一种开放式协议，它使用 TCP/IP 来提供对那些支持 X.500 模型的目录的访问，并且不像更为复杂的 X.500 目录访问协议 (DAP) 那样具有资源需求。例如，可以使用 LDAP 在因特网或内部网目录中查找人员、组织和其他资源。

(R)

日志源 (log source)
这是事件日志所来源于的安全设备或网络设备。

日志源扩展 (log source extension)
这是一种 XML 文件，它包含对事件有效内容中的事件进行标识和分类所需的所有正则表达式模式。

入侵防御系统 (intrusion prevention system, IPS)
这是一种系统，用于尝试拒绝潜在的恶意活动。拒绝机制可能涉及过滤、跟踪或设置速率限制。

入侵检测系统 (intrusion detection system, IDS)
这是一种软件，用于检测对网络或主机系统中的受监视资源进行的攻击尝试或成功攻击。

(S)

扫描程序 (scanner)
在 Web 应用程序中搜索软件漏洞的自动执行的安全程序。

设备支持模块 (Device Support Module, DSM)
这是一个配置文件，用于解析从多个日志源接收到的事件，并将这些事件转换为可以显示为输出的标准分类法格式。

身份 (identity)
这是来自数据源的属性集合，这些属性表示人员、组织、场所或项。

实时扫描 (live scan)
基于会话名称从扫描结果生成报告数据的漏洞扫描。

数据点 (datapoint)
这是在某个时间点计算而得的度量值。

数据库叶对象 (database leaf object)
这是数据库层次结构中的终端对象或节点。

刷新计时器 (refresh timer)
这是手动触发或者按指定时间间隔自动触发的内部设备，用于更新当前网络活动数据。

(T)

通用漏洞评分系统 (Common Vulnerability Scoring System, CVSS)
这是一个评分系统，用于对漏洞的严重性进行测量。

(W)

外部扫描装置 (external scanning appliance)
连接到网络以收集网络中资产的相关漏洞信息的机器。

网关 (gateway)
这是一种设备或程序，用于连接具有不同网络体系结构的网络或系统。

网络层 (network layer)
在 OSI 体系结构中，这是一个层，它提供用于在开放式系统与可预测服务质量之间建立路径的服务。

网络层次结构 (network hierarchy)
这是一种容器，用作网络对象的分层集合。

网络地址转换 (Network Address Translation, NAT)
在防火墙中，这是从安全因特网协议 (IP) 地址到外部注册地址的转换。这将启用与外部网络的通信，但屏蔽防火墙内侧使用的 IP 地址。

网络对象 (network object)
这是网络层次结构的一个组件。

违例 (violation)
这是绕过或违反企业策略的行为。

无类域间路由 (Classless Inter-Domain Routing, CIDR)
这是用于添加 C 类因特网协议 (IP) 地址的方法。这些地址提供给因特网服务提供商 (ISP)，以供其客户使用。CIDR 地址减小了路由表的大小，并使更多 IP 地址在组织内可用。

误报 (false positive)
这是分类为肯定（表示站点易受攻击），但用户确定实际为否定（不是漏洞，不易受攻击）的测试结果。

(X)

系统视图 (system view)
这是对构成系统的主要主机和受管主机的可视表示。

相关性 (relevance)
这是对网络中事件、类别或攻击的相对影响的测量。

协议 (protocol)
这是一组规则，用于控制通信网络中两个或两个以上设备或系统之间的通信和数据传输。

信任库文件 (truststore file)
包含可信实体的公用密钥的密钥数据库文件。

行为 (behavior)
这是操作或事件的可观察效果，包括其结果。

(Y)

严重性 (severity)
这是源对目标产生的相对威胁的测量。

叶 (leaf)
在树中，这是没有子代的条目或节点。

异常 (anomaly)
这是与网络的预期行为的偏差。

因特网服务提供商 (Internet service provider, ISP)
这是提供因特网访问的组织。

因特网控制报文协议 (Internet Control Message Protocol, ICMP)
这是一种因特网协议，网关使用此协议与源主机进行通信，例如报告数据报中的错误。

因特网协议 (Internet Protocol, IP)
这是一种协议，用于通过网络或互连网络路由数据。此协议充当较高协议层与物理网络之间的中介。另见传输控制协议 (Transmission Control Protocol)。

引用表 (reference table)
在这个表中，数据记录将已分配类型的键映射到其他键，然后将映射到的这些键映射到单一值。

引用集 (reference set)
这是网络上的事件或流派生的单一元素的列表。例如，IP 地址列表或用户名列表。

引用映射 (reference map)
这是将一个键直接映射到一个值的数据记录。例如，将一个用户名直接映射到一个全局标识。

应用程序特征符 (application signature)
这是一组唯一字符，这些字符通过检查包有效内容而获得，用于标识特定应用程序。

映射的引用映射 (reference map of maps)
这是将两个键映射到多个值的数据记录。例如，将应用程序的总字节数映射到源 IP。

有效内容数据 (payload data)
这是 IP 流中包含的除头信息和管理信息以外的应用程序数据。

域名系统 (Domain Name System, DNS)
这是一种分布式数据库系统，用于将域名映射到 IP 地址。

(Z)

侦察 (recon)
参见侦察 (reconnaissance, recon)。

侦察 (reconnaissance, recon)
收集与网络资源身份有关的信息的方法。将网络扫描和其他方法用于编译网络资源事件列表并为其分配严重性级别。

主机上下文 (host context)
这是一项服务，用于监视组件，以确保各个组件按预期方式操作。

主要 HA 主机 (primary HA host)
这是连接到 HA 集群的主计算机。

转发目标 (forwarding destination)
这是一个或多个供应商系统，用于接收来自日志源和流源的原始规范化数据。

资产 (asset)
在运营环境中已部署或将要部署的可管理对象。

子搜索 (sub-search)
这是一种功能，它允许在一组已完成的搜索结果中执行搜索查询。

子网 (subnet)
参见子网 (subnetwork)。

子网 (subnetwork, subnet)
这是划分为较小的独立子组（这些子组仍然互连）的网络。

子网掩码 (subnet mask)
对于因特网子网划分，这是一个 32 位掩码，用于标识 IP 地址的主机部分中的子网地址位。

自治系统号 (autonomous system number, ASN)
在 TCP/IP 中，这是由分配 IP 地址的中央权威机构分配给自治系统的编号。自治系统号使自动化路由算法能够区分自治系统。

A

ARP 重定向 (ARP Redirect)
这是一种 ARP 方法，用于在网络中存在问题时通知主机。

ARP
参见地址解析协议 (Address Resolution Protocol)。

ASN
参见自治系统号 (autonomous system number)。

C

CIDR
参见无类域间路由 (Classless Inter-Domain Routing)。

CVSS
参见通用漏洞评分系统 (Common Vulnerability Scoring System)。

D

DHCP
参见动态主机配置协议 (Dynamic Host Configuration Protocol)。

DNS
参见域名系统 (Domain Name System)。

DSM
参见设备支持模块 (Device Support Module)。

F

FQDN
参见标准域名 (fully qualified domain name)。

FQNN
参见标准网络名称 (fully qualified network name)。

H

HA 集群 (HA cluster)
这是一种高可用性配置，其中包含主服务器和一个辅助服务器。

HA
参见高可用性 (high availability)。

HMAC
参见基于散列的消息认证代码 (Hash-Based Message Authentication Code)。

I

ICMP
参见因特网控制报文协议 (Internet Control Message Protocol)。

IDS
参见入侵检测系统 (intrusion detection system)。

IP 多点广播 (IP multicast)
这是一种传输方式，即，将因特网协议 (IP) 数据报传输到单个多点广播组中的一组系统。

IP
参见因特网协议 (Internet Protocol)。

IPS
参见入侵防御系统 (intrusion prevention system)。

ISP
参见因特网服务提供商 (Internet service provider)。

L

L2L
参见从本地到本地 (Local To Local)。

L2R
参见从本地到远程 (Local To Remote)。

LAN
参见局域网 (local area network)。

LDAP
参见轻量级目录访问协议 (Lightweight Directory Access Protocol)。

M

Magistrate
这是一个内部组件，用于根据已定义的定制规则对网络流量和安全事件进行分析。

N

NAT
参见网络地址转换 (Network Address Translation)。

NetFlow
这是一种 Cisco 网络协议，用于监视网络流量流数据。NetFlow 数据包括客户机和服务器信息、使用的端口以及通过连接到网络的交换机和路由器流动的字节数和包数。这些数据将发送到 NetFlow 收集器，数据分析在该位置执行。

O

OSI
参见开放式系统互连 (open systems interconnection)。

OSVDB
参见开放式源代码漏洞数据库 (Open Source Vulnerability Database)。

Q

QID 映射 (QID Map)
这是一种分类法，用于标识各个唯一事件，并将事件映射到低级别和高级别类别，从而确定事件的关联方式和组织方式。

R

R2L
参见从远程到本地 (Remote To Local)。

R2R
参见从远程到远程 (Remote To Remote)。

S

SNMP
参见简单网络管理协议 (Simple Network Management Protocol)。

SOAP
这是一种基于 XML 的轻量级协议，用于在分散的分布式环境中交换信息。使用 SOAP 可以通过因特网查询和返回信息以及调用服务。

T

TCP
参见传输控制协议 (Transmission Control Protocol)。

W

Whois 服务器 (whois server)
这是一种服务器，用于检索有关已注册的因特网资源的信息，例如域名和 IP 地址分配。

索引

[Z]

C

D

F

I

J

N

P

S

T

V

[特别字符]