IBM Security QRadar
V 7.3.0

新增内容

备注

使用此信息及其支持的产品前，请阅读第 17 页的『声明』中的信息。

产品信息

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

目录

QRadar 系列产品新增内容简介

管理员查看 IBM® Security QRadar® 的新增功能以帮助确定是否升级、为其支持的用户计划培训以及了解新增功能。

目标受众

本指南旨在用于负责调查和管理网络安全的现有 QRadar 用户。

技术文档

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

有关如何访问 QRadar 产品库中更多技术文档的信息，请参阅访问 IBM Security 文档技术说明 (www.ibm.com/support/docview.wss?rs=0&uid=swg21614644)。

联系客户支持

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)。

关于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，并且没有任何一种产品、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、产品和服务设计为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：

此程序的使用可能涉及各种法律或法规，包括与隐私、数据保护、雇佣以及电子通信和存储有关的法律或法规。IBM Security QRadar 只能用于合法目的并且只能以合法方式使用。客户同意按照适用的法律、法规和政策使用本程序，并承担遵守适用的法律、法规和政策的所有责任。被许可方表示将获取或已获取允许合法使用 IBM Security QRadar 所需的任何许可、许可权或许可证。

QRadar V7.3.0 中的新增功能

IBM Security QRadar V7.3.0 系列产品包含新的搜索分析，简化了已部署主机的迁移，并缩短了部署时间，改进了性能，提高了平台安全性等等。

当今网络越来越大，也越加复杂，保护网络不受恶意攻击者的侵害是一项永远不会结束的任务。寻求保护知识产权、保护其客户身份、避免业务中断的组织不仅仅需要监视日志和网络流数据；他们需要利用易于使用的先进解决方案来快速检测安全性攻击并采取操作。

IBM Security QRadar 可以充当小型、中型或大型组织的安全运营中心中的锚点解决方案，以凭借多年的上下文洞察价值来收集、标准化和关联网络数据。它还与许多其他产品集成，提供对本地部署、混合与云环境中安全事件的完整的统一化可视性。

QRadar

IBM Security QRadar V7.3.0 系列产品包含新的搜索分析，简化了已部署主机的迁移，缩短了部署时间，改进了性能，提高了平台安全性等等。

QRadar 核心功能

IBM Security QRadar 核心功能已使用更灵活的容量管理和部署选择、更多租户用户功能和改进的安装、许可发放和软件修补进行了增强。

不再需要激活密钥

在 QRadar V7.3.0 安装期间，您从列表中选择要安装的设备类型。在前发行版中，安装者在安装过程期间手动为设备输入激活密钥。

有关安装 QRadar 的更多信息，请参阅*IBM Security QRadar Installation Guide*。

移除日志源限制

对 QRadar V7.3.0 中许可发放模型的改进使您更容易管理日志源。日志源限制已被移除，您不再需要为日志源购买许可证。

在升级到 QRadar V7.3.0 时，先前日志源限制已被移除。

有关 QRadar 许可证的更多信息，请参阅《*IBM Security QRadar Administration Guide*》中的『管理许可证』一章。

轻松地在部署中分配事件和流容量

通过为部署中的任意主机分配每秒事件数 (EPS) 和每分钟流量 (FPM)，而不考虑将许可证分配到哪一台主机，从而适应工作负载变化。

各个许可证的 EPS 和 FPM 现在已汇总到共享许可证池中。作为管理员，您可以使用新的**许可证池管理**窗口来快速查看部署中的累积 EPS 和 FPM 容量，并确定将 EPS 和 FPM 分配给受管主机的最佳方法。

例如，您具有一个 QRadar V7.2.8 分布式部署，其中包含两个事件处理器，一个具有 7,500 EPS，另一个具有 15,000 EPS。在升级到 QRadar V7.3.0 时，每个处理器都保持升级前的 EPS 分配，但加总的 22,500 EPS 成为共享许可证池的一部分。当事件处理器的数据量发生变化时，或者当您添加受管主机时，您可以重新分配 EPS 容量。

有关管理共享许可证池的更多信息，请参阅*IBM Security QRadar Administration Guide* 中的『许可证管理』一章。

更安全的操作系统和灵活的磁盘分区 (LVM)

QRadar 在支持逻辑卷管理器的 Red Hat Enterprise Linux V7.3 上运行，因此您可以创建分区和调整分区大小，并将存储集群汇总到一起。

例如，您的虚拟机上具有 QRadar All-In-One，而您需要更多本地磁盘空间，以便能够将事件存储更长时间。可以添加另一个磁盘来扩展 /store 分区。

此外，在 Red Hat Enterprise Linux V7.3 中，**service** 命令将替换为 **systemctl** 命令。使用脚本管理 QRadar 部署的管理员必须复查和更新脚本。

例如，更新脚本以将旧命令 service <*service_name*> start|stop|restart 替换为新命令 systemctl start|stop|restart <*service_name*>。

有关使用 **systemctl** 命令的更多信息，请参阅 Red Hat Enterprise Linux V7 文档。

安全性更新

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

在通过代理服务器进行自动更新时，更新缺省 CA 证书的步骤稍有变化。

租户用户可以创建定制属性

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的信息，而无需受管安全性服务提供程序 (MSSP) 管理员的协助。通过此功能，租户用户可以查看和搜索 QRadar 通常不会标准化和显示的数据。

作为 MSSP 管理员，您具有对租户用户创建的所有定制属性的写许可权。如果规则和报告中频繁使用属性，可以优化租户的定制属性以改善搜索性能。租户用户不能优化自己创建的属性。

有关处理定制事件和流属性的信息，请参阅《*IBM Security QRadar* 用户指南》。

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 管理员创建的参考数据。现在，在 V7.3.0 中，具有**代理管理** > **管理参考数据**用户角色的租户用户可以创建和观来自己的参考数据集合，而无需 MSSP 管理员协助。

凭借此功能，租户用户可以跟踪业务数据或来自外部源的数据，并且可以在 QRadar 搜索、过滤、规则测试条件和规则响应中参考这些数据。例如，包含已终止合同员工的用户标识的参考集可以用于防止员工登录网络。

有关处理参考数据集合的更多信息，请参阅《*IBM Security QRadar Administration Guide*》

Master Console 和 Deployment Editor 已被移除

虽然 Master Console 不会随着 QRadar V7.3.0 一起安装，但您可以与 QRadar V7.2.8 一起发布的 使用 Master Console V0.11.0 来监视 QRadar V7.3.0 部署。

有关安装 Master Console 的更多信息，请参阅 *IBM Security QRadar Master Console Guide*。

不依赖于 Java™ 的 System and License Management 将取代 Deployment Editor。

有关管理 QRadar 部署的更多信息，请参阅《*IBM Security QRadar Administration Guide*》中的『系统管理』一章。

高可用性 (HA)

IBM Security QRadar V7.3.0 引入了一种技术，能够在对高可用性事件收集器应用软件修订时尽量缩短停机时间。

向高可用性事件收集器应用软件修订时缩短停机时间

在对一对高可用性事件处理器应用软件修订时，将使用能够所选停机时间的新集群技术。该集群技术能够尽量降低对数据收集过程的影响。

设备

IBM Security QRadar V7.3.0 引入了高性能设备、专用于网络包捕获的设备以及实时重构网络会话的设备，提供了更详细的威胁可视性。

QRadar xx29

IBM Security QRadar xx29 (MTM 4412-Q2A) 设备是任何 xx28 设备的 M5 版本。例如，您可以使用 QRadar xx29 作为 QRadar Event Processor 1629、QRadar Flow Processor 1729、QRadar 3129 (All-in-One) 等等。

有关更多信息，请参阅 *QRadar Hardware Guide*。

QRadar xx48

IBM Security QRadar xx48 (MTM 4412-Q3B) 为需要更高级别性能的企业客户机捕获更大的流量卷。通过 QRadar xx48 更快速的数据处理功能、数据可以更快地用于搜索和分析，以及能够支持更多启用了 IP 的设备，您可以使用更少的设备，因此节省机架空间。

有关更多信息，请参阅 *QRadar Hardware Guide*。

QRadar Network Packet Capture

IBM Security QRadar Network Packet Capture (MTM 4412-F2C) 提供更多存储容量以使用户能够将更多包数据存储更长的时间，并提高了性能。QRadar Network Packet Capture 设备还提供了更多捕获端口和额外的配置灵活性，以支持多种部署选项。

有关更多信息，请参阅 *QRadar Hardware Guide*。

QRadar Network Insights

IBM Security QRadar Network Insights (MTM 4412-F3F) 设备可以提供详细的网络流分析，以扩展 QRadar 的威胁检测功能。QRadar Network Insights 实时重构网络会话，收集具有高价值的指示符，并分析元数据和内容。

有关更多信息，请参阅 *QRadar Hardware Guide*。

RESTful API

IBM Security QRadar V7.3.0 引入了 API 端点的 V8.0 版本。

新端点

QRadar V7.3.0 引入了许多新类别的 API 端点并更新了以下类别中的现有端点：

分析 API 端点

构建块

定制规则

配置 API 端点

主机

许可证池

远程网络

远程服务

GUI 应用框架端点

命名服务

已登台配置 API 端点

许可证池

远程网络

远程服务

服务端点

DNS 查找

DIG 查找

WHOIS 查找

有关更多信息，请参阅 *IBM Security QRadar API Guide*。

Ariel Query Language (AQL)

IBM Security QRadar 引入了新 AQL 函数和增强功能。

将相关事件分组到一起以便更清楚地了解网络和用户活动

使用新的 AQL 事务会话来轻松地跟踪网络和用户活动。

您可以使用 AQL 事务序列将上下文相关事件分组到自己的唯一会话中。这些会话显示了事件序列和后续结果。例如，您可以看到某人登录的时长，或者是否曾有任何未经授权的登录尝试。

有关更多信息，请参阅 *IBM Security QRadar Ariel Query Language Guide*。

将网络地址与主机地址区分开来以增强搜索的过滤功能

对 AQL 使用按位运算符来屏蔽 IP 地址和优化 IP 地址搜索条件。

您可以返回特定网络分段的所有 IP 地址，也可以返回具有特定 IP 地址的设备。您可以过滤对 IP 地址八位元的任意或所有四个八位元的搜索。例如，您可以使用按位 AND 运算符来搜索与 xxx.100.xxx.xxx 匹配的所有 IP 地址，以查看一组特定的 IP 地址。您可以使用 LONG 函数将 IP 地址转换为长整型整数，以便能够在按位运算中使用。

有关更多信息，请参阅 *IBM Security QRadar Ariel Query Language Guide*。

QRadar 应用程序

在 IBM Security QRadar V7.3.0 中，如果应用程序能够访问更多内存和存储空间，使用应用程序节点设备来改善应用程序的性能。

客户、开发者和业务合作伙伴使用 IBM Security App Exchange 来共享安全性应用程序和内容扩展以增强 IBM Security 产品。

改善了应用程序的处理能力

在前发行版中，在设置 GUI 应用程序框架时，应用程序在 QRadar Console 上运行，且资源限制会影响所部署的每个应用程序。在 QRadar V7.3.0 中，您可以在自己的计算机硬件上部署专用应用程序节点，以缓解 QRadar 运行应用程序所需的系统资源的负载。

有关配置应用程序节点的更多信息，请参阅《*IBM Security QRadar Administration Guide*》。

应用程序通信以提供更清晰的威胁检测和洞察

通过发布 API，应用程序允许其他应用程序使用自己提供的情报和值，以便实现增强的安全性。

例如，当提供威胁情报订阅源的应用程序发布其 API 时，恶意软件检测引擎应用程序可以在自己的应用程序中使用该威胁情报订阅源数据。

优化的应用程序备份和恢复过程

应用程序配置现在可以独立于应用程序数据进行备份和复原。

应用程序配置作为夜间配置备份的一部分进行备份。配置备份包括 QRadar Console 和应用程序节点上安装的应用程序。在复原备份时，可以选择**安装的应用程序配置**选项来复原应用程序配置。

通过使用夜间运行的易于使用的脚本，可独立于应用程序配置来备份应用程序数据。还可以使用该脚本复原应用程序数据，并配置备份时间和数据保留期。

有关备份应用程序和应用程序数据的更多信息，请参阅《*IBM Security QRadar Administration Guide*》。

QRadar Vulnerability Manager 和 QRadar Risk Manager

在 IBM Security QRadar Vulnerability Manager V7.3.0 中，您可以优化在资产上发现服务的速度和准确性。

资产上的服务发现的性能改进

要改进资产上的服务发现的性能和准确性，现在可以配置参数（例如，超时和重试次数）来适应网络速度和基础结构。

管理漏洞性能改进

SQL 查询和搜索过滤器已经过调优，现在**管理漏洞**、**按实例**、**按漏洞**和**按资产**屏幕上的性能已有所改善。当有大量资产和漏洞时，这一改进尤为明显，可伸缩性和易用性有所提高。

QRadar Incident Forensics

IBM Security QRadar Incident Forensics V7.3.0 引入了高级恢复选项和 IBM QRadar Network Packet Capture 故障诊断信息以帮助您解决常见问题。

可用于 QRadar Incident Forensics 恢复的 PCAP 设备选择

在运行 QRadar Incident Forensics 恢复时，要仅查看来自部署中的 PCAP 设备的流量，请选择**定制捕获设备**。

有关更多信息，请参阅《IBM Security QRadar Incident Forensics 用户指南》。

提供了更多故障诊断信息以帮助您快速确定并解决问题

包含如何配置日期和时间以及用于配置 QRadar Network Packet Capture 中的加速键端口设置的其他信息和 Python 分流和分块 API 示例。

有关更多信息，请参阅《IBM QRadar Network Packet Capture 管理指南》和《IBM QRadar Network Packet Capture API 指南》。

QRadar Network Insights

IBM QRadar Network Insights V7.3.0 引入了对 TLV (tab-length-value) 格式的支持。

可供 QRadar Network Insights 使用的 TLV 选项

使用 QFlow 收集器以 TLV (tab-length-value) 格式将数据导出到 QFlow Processor。对于新 IBM Security QRadar安装，或部署中不包含 QRadar Network Insights 设备的 QRadar 升级，从 **QFlow 格式**菜单中选择 TLV 格式。

有关更多信息，请参阅《IBM Security QRadar Incident Forensics 管理指南》。

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 可能在其他国家或地区不提供本文档中讨论的产品、服务或功能特性。 有关您所在区域当前可获得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暗示只能使用 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（无论是明示的还是暗含的）保证，包括但不限于暗含的有关非侵权、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暗含的保证。 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。

本信息中对任何非 IBM Web 站点的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 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。

提供的性能数据和引用的客户机示例，仅供参考。实际的性能结果可能有所不同，具体取决于特定配置和操作条件。

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。 所有这些名称均是虚构的，如与实际人员或商业企业有任何相似之处，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。当前的 IBM 商标泪飙，可从 Web 站点 www.ibm.com/legal/copytrade.shtml 上的 "版权和商标信息"部分获取。

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。

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。

产品条款和条件文档

只要遵守下列条款和条件，即授予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 的明示同意，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。

商业性使用

您仅可在贵公司内部复制、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，无论明示的还是暗含的。

只要 IBM 认为这些出版物的使用会损害其利益或者 IBM 判定未正确遵守上述指示信息，IBM 将有权撤销本文授予的许可权。

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（无论是明示的还是暗含的）保证，包括但不限于暗含的有关适销、非侵权和适用于某种特定用途的保证。

IBM 网上隐私声明

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

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

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

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

Printed in China