IBM QRadar on Cloud

本“服务描述”描述云服务。适用的订单文档提供有关客户订单的定价和其他详细信息。

1. 云服务

1.1 服务产品

客户可以从以下可用服务产品中选择

1.1.1 IBM QRadar on Cloud

IBM QRadar on Cloud 服务产品从 IBM Cloud 提供基于 IBM Security QRadar SIEM 产品的高级安全情报解决方案。它允许客户收集、关联和存储内部环境和云环境生成的事件，并且像使用内部部署的 QRadar SIEM 产品一样执行安全和威胁管理。作为服务产品的一部分，IBM 还提供全天候基础架构监视，并随时应用最新软件版本级别或关键补丁。

此云服务包含九十 (90) 天的有效、可搜索的存储，并以每秒 100 个事件 (EPS) 的数量授予权限。

1.2 可选服务

1.2.1 IBM QRadar on Cloud Temporary Upgrade

此升级服务为收集和处理日志事件额外提供 1,000 EPS 容量，但服务时间仅为短暂的几个月。客户可购买多个升级服务单元，可多达该服务产品能够支持的最大 EPS 级别。这部分服务的目的是使客户通过临时容量升级，满足年内“峰值”时刻的容量需求。该服务期限结束时，将从客户环境中移除这些临时增加的容量。

1.2.2 IBM QRadar on Cloud Data Capacity

数据容量升级将添加额外的存储器并扩展分析期。每购买 100 EPS 的升级，容量升级向客户提供长达 1 整年存储的事件数据。

1.2.3 IBM QRadar on Cloud Flows Add-On

与 IBM QRadar SIEM 和流处理器集成，提供第 3 层网络可视性和流分析，帮助客户感知、检测和响应整个客户网络中的活动。

此云服务包含九十 (90) 天的有效、可搜索的存储，并以每分钟 10,000 个流 (FPM) 的数量授予权限。

1.2.4 IBM QRadar on Cloud Vulnerability Management Add-On

主动感知和发现网络设备以及应用程序安全漏洞，添加上下文并且支持划分修补和缓解活动的优先级。

1.2.5 IBM QRadar on Cloud Log Archival

允许客户在订购期内归档来自云服务的事件数据。IBM 将与客户共同将指定的事件写入对象存储器，以便进行归档。根据客户的请求，IBM 将在此类请求提出后的三 (3) 个工作日内向客户的云服务实例重新提交最多三十天的已存档事件数据。此类数据将可供客户使用 48 小时，之后将会被返回到归档对象存储器。客户每三个月最多可以提出两次请求。每购买 100 EPS 的升级，容量升级向客户提供最多 1 整年存储数据。

1.2.6 IBM QRadar on Cloud Flows Add-On Data Capacity

通过每购买 10,000 FPM 的升级，向客户提供最多 1 整年存储流数据，数据容量升级将添加额外的存储器并扩展分析期。

1.2.7 IBM QRadar on Cloud Flows Add-On Log Archival

该服务产品允许客户在订购期内归档来自云服务的流数据。IBM 将与客户共同将指定的流记录写入对象存储器，以便进行归档。根据客户的请求，IBM 将在此类请求提出后的三 (3) 个工作日内向客户的云服务实例重新提交最多三十天的已存档流数据。此类数据将可供客户使用 48 小时，之后将会被返回到归档对象存储器。客户每三个月最多可以提出两次请求。每购买 10,000 FPM 的升级，容量升级向客户提供最多 1 整年存储数据。

1.2.8 IBM QRadar on Cloud for Non-Production Environment

IBM QRadar on Cloud for Non-Production Environment 服务产品交付了云服务的专用测试实例。它允许客户收集、关联和存储内部环境和云环境生成的事件，并且像在专用测试环境中 使用内部部署的 QRadar SIEM 产品一样执行安全和威胁管理。作为服务产品的一部分，IBM 还提供全天候基础架构监视，并随时应用最新软件版本级别或关键补丁。客户只能将此云服务用于非生产测试目的。

此云服务包含九十 (90) 天的有效、可搜索的存储。

1.3 加速服务

1.3.1 IBM QRadar on Cloud Optimization Service

对于此远程交付的订购服务，IBM 将与客户召开评审会议，以评估客户的云服务实例的当前运行状况，并通过 QRadar on Cloud 运行状况报告将结果交付给客户，报告中将确定需改进的方面（如果有）。

另外，根据客户的请求，IBM 将在一年时间内向客户提供最多八 (8) 天的以下任何咨询服务。

- 协助将其他日志源添加到；
- 配置其他搜索、报告和仪表板；
- 对现有 QRadar 部署执行其他调优；以及
- 提供有关相关 QRadar 主题的知识传授。

1.3.2 设置服务

以下设置服务以远程方式交付并且可单独订购。无论是否用尽了小时数（如果适用），订购的每项服务自订购之日起 90 天后到期，除非另有说明。服务将包含一名指定的 IBM 服务项目经理，负责安排任何启动电话会议。

a. **IBM QRadar on Cloud Deployment Services**

该服务提供四十 (40) 小时的专业服务，期间 IBM 将执行以下部分或所有操作：

IBM 将在期间开展最长 16 小时的 SIEM 体系结构评审，以定义客户的报告需求，并且将在解决方案体系结构报告中将评审结果交付给客户，上述结果将帮助定义和捕获客户需求。

此报告将包括：

- 客户定义的报告需求，用于帮助满足客户的合规性、审计和安全情报需求。
- IBM 可协助实施的安全情报需求、用例和应用程序（最多十 (10) 个用例和最多 (2) 个应用程序）。
- 有关支持用例时需要的客户日志和流源的高层次信息。
- 网络基础架构注意事项，如防火墙和端口。

如果剩余时间允许，基于解决方案体系结构报告，IBM 将执行以下任务：

- 将最多十 (10) 个日志源类型的最多三 (3) 个实例的事件集合配置到云服务中。该活动包含将知识传授给客户的相关人员，这样他们可以根据需要添加更多日志源。只有标准 QRadar 设备支持模块 (DSM) 支持的日志源才会作为该服务的一部分包含在内。
- 初始调优，包括 a) 激活开箱即用规则、保存的搜索、累计时间序列图和报告；b) 确定并消除噪音源；c) 通过 NFS、CIFS 或 iSCSI 配置脱机存储器。
- 通过解决方案体系结构文档中记录的 IBM QRadar App Exchange 来实施十 (10) 个用例和两 (2) 个应用程序。

b. **IBM QRadar on Cloud Custom Parser Service**

该服务将提供单个定制解析器/uDSM 的开发，以支持将发送至云服务的客户的非标准日志源类型，并且包含以下任务：

- 为一种非标准日志源类型创建定制解析器（远程执行工作）；
- 创建、配置和映射 uDSM；
- 部署和测试定制 uDSM；以及
- 解析日志源的最多二十五种消息类型。

2. 数据处理和保护数据表

位于 http://ibm.com/dpa 的 IBM 数据处理附录 (DPA) 以及下面链接中的“数据处理和保护数据表”（称为数据表或 DPA 附录）提供针对云服务及其选项的其他数据保护信息，关于可处理的内容类型、所涉及的处理活动、数据保护功能以及有关内容保留和返回的细节。如果 i) 欧盟通用数据保护条例 (EU/2016/679) (GDPR)；或 ii) http://ibm.com/dpa/dpl 上标示的其他数据保护法律适用于内容中包含的个人数据，那么 DPA 也适用于这些个人数据。

https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=FB0F42F0750011E6865BC3F213DB63F7

3. 服务级别和技术支持

3.1 服务标准协议

IBM 为客户提供以下可用性服务级别协议 (SLA)。IBM 会根据累积的可用云服务应用适用的最高赔偿，如下表中所示。可用性百分比的计算方法为：“约定的月份”内总分钟数减去“约定的月份”内服务停用的总分钟数，再除以“约定的月份”内总分钟数。“服务停用”定义、索赔过程以及如何联系 IBM 反馈服务可用性问题在 IBM 的云服务支持手册 (https://www.ibm.com/software/support/saas_support_overview.html) 中进行了说明。

可用性	积分 （每月订购费用的百分比*）
小于 99.9%	2%
低于 99.0%	5%
低于 95.0%	10%

* 订购费用是当月该索赔相关的合同价格。

3.2 技术支持

通过在位于 https://www.ibm.com/support/home/pages/support-guide/ 的 IBM 支持指南中选择云服务来查找针对云服务的技术支持，包括支持联系人详细信息、严重性级别、可用性的支持小时数、响应时间以及其他支持信息和流程。

4. 费用

4.1 收费标准

云服务的收费标准在交易文档中指定。

以下收费标准适用于此云服务：

- 互动是与云服务相关的专业或培训服务。
- “每秒事件数”是指每秒出现一次通过使用云服务处理或者与使用云服务相关的特定事件。
- “每分钟流数”是指云服务管理或处理的每分钟流数。一个流是两个主机之间的一个通信记录。包含相同源 IP、目标 IP、源端口、目标端口和协议的包将组合为一条流记录。
- 资产是由云服务访问或管理的唯一标识的有形资源或价值项。

5. 附加条款

对于 2019 年 1 月 1 日之前执行的云服务协议（或等效的基础云协议），可用的条款 (https://www.ibm.com/acs) 将适用。

5.1 支持软件

根据以下条款向客户提供支持软件：

支持软件	适用的许可条款（如果有）
数据网关	客户最多只能安装和使用十 (10) 个数据网关的副本