

IBM Intelligent Operations Center for Emergency Management on Cloud

本“服务描述”描述 IBM 向客户提供的 Cloud Service。客户表示公司、公司授权用户和 Cloud Service 接收方。提供适用的“报价”和“权利证明”(PoE) 作为独立的交易文档。

1. Cloud Service

IBM Intelligent Operations Center for Emergency Management on Cloud 是一款事件和紧急情况管理解决方案，用于日常运营以及紧急或危急情况。其集成并关联多个信息源以创建动态的公共地理运营图和基于分析的洞察，帮助事件指挥人员和紧急事务管理人员了解并快速适应不断变化的情况。

通过将当前运营状态知识与影响分析功能相组合，并提供近乎实时的地理空间框架信息，Intelligent Operations Center for Emergency Management on Cloud 帮助向一线人员、事件指挥人员、安全负责人、各类项目干系人以及管理人员或政府领导提供命令和控制功能。

基本功能：

- Intelligent Operations Center 控制台支持 Cloud Service 用户查看事件和事件状态、地理空间信息（需要集成到地理信息系统 - GIS 服务器，未随 Cloud Service 一起提供），以及发布用于管理关键绩效指标 (KPI)/任务的报告。
- 支持 Cloud Service 用户基于时间和位置查看地图上 Cloud Service 处理的事件或其他数据的关联。
- 支持 Cloud Service 用户基于 Cloud Service 处理的数据的阈值引发事件。
- 支持 Cloud Service 用户在 IOC 控制台中查看有关捕获的事件或其他数据的报告。
- 支持 Cloud Service 用户在 IOC 控制台中基于捕获的事件或其他数据查看 KPI/任务。
- Cloud Service 用户可以执行标准操作过程 (SOP)/工作流程，帮助自动化对事件、KPI/任务阈值或报告中所定义条件的标准响应。
- 使用主管仪表盘，这是一个专门的界面，为 Cloud Service 用户提供有关城市中所有事件的一览摘要信息。
- 使用具有专门的命令中心界面的工作站客户机，这为 Cloud Service 用户提供丰富的图形用户界面 (GUI) 功能以用于情境感知和事件/紧急情况管理，并且支持使用多屏和视频墙显示器。
- Cloud Service 用户可处理警报通知（任何值得注意的报告或事件将通过其数据订阅源传输至软件）并在其地理空间上下文中的画布上显示这些警报。用户还可以手动将警报和相关信息插入画布上适合的位置。
- Cloud Service 支持用户将相关警报分组到事件：一个警报表示一条信息的报告，而事件表示应在系统中进行跟踪的持续发生的事件。Cloud Service 可帮助用户设置事件的操作状态，提供额外的注意事项以及附加感兴趣的文档。这允许多个 Cloud Service 用户协作并在呈现事件时展开事件的详细信息。
- 如果已指定多个事件，那么 Cloud Service 允许用户链接到这些事件，通过创建“事件状态视图”来区分模式是否存在。
- Cloud Service 提供基于角色的流程，此流程在后台运行以帮助根据预兆活动的发生识别可能出现的威胁/商机。
- “事件文件”工具支持 Cloud Service 用户指定事件相关信息集合，例如，资产、文档和链接。
- 威胁监视面板帮助 IBM SaaS 用户识别具有用户建立的符合条件的近似警报的所有功能和资产。可基于特定功能或资产、警报类型、感兴趣的领域以及与感兴趣的功能相关的警报近似值创建多个威胁概要文件。
- “任务就绪”工具支持 Cloud Service 用户创建和监控用户创建的多个目标的状态。借助“任务就绪”工具，如果资产更改会妨碍整体目标的达成，那么用户可接收到此类更改的即时通知。此工具支持用户向下钻取任务依赖关系，以查找存在风险的任务和资产及其伤害性质。
- 使用“战术数据层”协作工具以创建和共享以地图作为画布的标记层，例如，图样、注释或评论。

- 支持实时维护公共操作图像，同时根据“活动状态”公共操作图运行单独的“假设情况”模拟。
- 使用“影响分析工具”以切换到假设情况状态，并模拟各种紧急情况或灾难事件，例如，炸弹爆炸、风暴潮和强风。用户可使用内置模拟引擎来评估紧急情况或灾难事件的影响。
- 使用“决策支持工具”以帮助更好地理解 and 优化恢复过程。可基于资源可用性和定位以及恢复优先级运行恢复模拟。
- 使用“视线分析工具”（需要 Cloud Service 不提供的 3D 映射）以确定特定距离内以及任何指定地点直视范围内的位置。

1.1 IBM Intelligent Operations Center for Emergency Management Standard User on Cloud

标准用户可访问上述所有基本功能。

1.2 IBM Intelligent Operations Center for Emergency Management Premium User on Cloud

高级用户可访问上述所有基本功能以及以下高级用户功能：

- 针对其环境创建和修改 KPI/任务以及报告。
- 创建和修改资产基础结构及其内部依赖关系和环境报告。
- 创建和修改与其环境相关的 SOP 和工作流程。
- 创建和修改选项卡、视图和其他可视演示文稿。
- IT 管理人员可通过管理界面管理 Cloud Service。
- 通过集成 API 从客户和第三方系统导入数据。
- 配置分析，以根据时间和位置发现事件和资产之间的关联。
- 定义和管理界面

1.3 IBM Intelligent Operations Center for Emergency Management Consumer User on Cloud

使用者用户可查看只读数据/报告、提交服务请求，以及查看请求的状态。使用者用户无权访问基本功能或任何标准用户或高级用户功能。

1.4 IBM Intelligent Operations Center for Emergency Management Mobile User on Cloud

移动用户无权访问基本功能或任何标准用户或高级用户功能，以下除外：

- 针对移动用户提供移动 HTML5 界面以与命令中心人员或其他移动用户进行双向协作，并共享公共操作图。
- 移动用户可通过移动设备在系统中添加文本信息、视频和照片。
- 在创建事件时，移动设备上的移动用户可快速将收集的信息直接添加到事件日志。
- 移动用户可开启和关闭各种基于地图的层以定制其可视视图。视图可包含实时天气、警报和事件的位置、公共安全位置、公共安全资源（例如，消防栓）和其他关键基础结构。
- 移动用户可在创建和更新时实时查看战术数据层。
- 移动用户可选择资产并检查相关关键信息，例如，应急计划和蓝图。移动用户可查看资产状态变更。
- 移动用户可选择可用相机和查看其中的实时图像。
- 移动用户可从全局虚拟绑定程序访问和查看表单和文档。

2. 安全描述

此 Cloud Service 遵循 <https://www.ibm.com/cloud/resourcecenter/content/80> 中提供的针对 IBM SaaS 的 IBM 数据安全和隐私原则，以及本部分中提供的任何其他条款。对于 IBM 数据安全和隐私原则的任何更改都不会降低 Cloud Service 的安全性。

2.1 遵守法律

各方负责遵守：i) 适用于其业务和内容的法律和法规，以及 ii) 与进口、出口和经济制裁相关的法律和法规，包括那些美国的禁止或限制（无论直接或间接地）向（或为）特定国家、特定目的、特定最终用户出口、再出口、转让产品、技术、服务或数据的法律和法规。

针对美国政府出口条例，确定此产品符合 License Exception ENC (740.17(b)(2))（以前称为 ENC Restricted）的资格。除禁运/恐怖主义国家或地区外，可以向所有非政府最终用户销售此产品。未事先获得美国政府出口核准，不得向以下国家或地区之外的政府最终用户销售此产品：美国、加拿大、澳大利亚、奥地利、比利时、保加利亚、塞浦路斯、捷克共和国、丹麦、爱沙尼亚、芬兰、法国、德国、希腊、匈牙利、冰岛、意大利、日本、拉脱维亚、立陶宛、卢森堡、马耳他、荷兰、新西兰、挪威、波兰、葡萄牙、罗马尼亚、斯洛文尼亚、斯洛伐克、西班牙、瑞典、瑞士、土耳其和英国。

2.2 受管控内容

此 Cloud Service 并非旨在满足任何受管控内容（例如，个人信息或敏感的个人信息）的特定安全要求。客户负责确定在客户使用的与 Cloud Service 有关的内容类型方面，此 Cloud Service 是否符合客户需求。

2.3 数据收集

客户了解并同意，作为 Cloud Service 正常运行和支持的一部分，IBM 可向客户（客户的员工和承包商）通过跟踪等技术收集有关 Cloud Service 使用的个人信息。IBM 公司以此收集 Cloud Service 的使用统计信息和有效性信息，旨在改善用户体验和/或定制与客户的交互。客户确认其将取得或已取得同意，允许 IBM 在遵守适用法律的情况下，在 IBM、其他 IBM 公司及其分包商内部处理收集到的个人信息用于上述目的，无论我们和我们的分包商在何处开展业务。IBM 将履行客户的员工和承包商访问、更新、纠正或删除所收集的个人信息请求。

3. 服务级别目标

此 Cloud Service 的服务级别目标为：

- 在常规安排的维护时间窗口之外达到 99.5% 的可用性。
- 最多 5 秒响应时间，表示正在进行 Web 页面活动。

服务级别目标是一个目标，并不构成对客户的保证。如果 IBM 未达到服务级别目标，将不向客户提供任何退款、积分或其他补偿。

4. 技术支持

通过位于以下地址的 IBM Client Success Portal 提供 Cloud Service 技术支持：

<https://support.ibmcloud.com>。IBM 将提供《IBM 软件即服务支持手册》，其中提供了技术支持联系信息以及其他信息和流程。技术支持随附于 Cloud Service，不作为独立产品提供。

严重性	严重性定义	支持期间的响应时间目标
1	关键业务影响/服务故障： 业务关键功能无法操作或关键接口出现故障。该内容通常适用于生产环境，表示无法访问服务对运营造成了巨大影响。该情况需要立即提供解决方案。	在 1 小时内
2	重大业务影响： 服务特性或服务功能在使用中受到严重限制，或者客户可能错过业务截止期限。	在 2 个工作小时之内
3	轻微业务影响： 表示服务或功能尚且可以使用，并不会对运营造成重大影响。	4 个工作小时之内
4	极小业务影响： 查询或非技术请求。	在 1 个工作日之内

5. 权利和计费信息

5.1 收费标准

Cloud Service 根据交易文档中指定的收费标准提供：

- a. **并发用户** - 获取 Cloud Service 时所采用的一种计量单位。并发用户是指在任何特定时间点访问 Cloud Service 的人员。不管该人员是否多次同时访问 Cloud Service，只会将该人员视为单个并发用户。客户必须为每位同时访问 Cloud Service 的“并发用户”获取一份权利，使其在客户权利证明 (PoE) 或交易文档中所指定的评估期间，能够以任何方式，通过任何途径，直接或间接地（例如：通过多路复用程序、设备或应用程序服务器）访问 Cloud Service。
- b. **合格参与者** - 获取 IBM SaaS 时所采用的一种计量单位。每个符合条件参与 Cloud Service 所管理或跟踪的任何服务交付计划的个人或实体都称为一个“合格参与者”。客户必须获得足够的权利，以涵盖在客户的“权利证明”(PoE) 或交易文档中所指定的评估期间在 Cloud Service 内管理或跟踪的所有合格参与者。

5.2 部分月度费用

交易文档中指定的部分月度费用可按比例进行评估。

5.3 盘盈费用

如果评估期间 Cloud Service 的实际使用超出了 PoE 中指定的权利，那么将按照交易文档中的规定向客户收取盘盈费用。

6. 期限和续约选项

Cloud Service 期限自 IBM 通知客户可访问 PoE 中记录的 Cloud Service 之日算起。PoE 将指定 Cloud Service 是自动续约、在持续使用基础上继续，还是在期限结束时终止。

对于自动续约，除非客户在期限到期日期之前，至少提前 90 天发出不再续约的书面通知，否则将按照 PoE 中指定的期限对 Cloud Service 自动续约。

对于持续使用，在客户提前 90 天发出终止书面通知之前，Cloud Service 将以月为单位继续有效。Cloud Service 的有效期将于 90 天期限过后的日历月末终止。