IBM Cloud Identity

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

IBM Cloud Identity 为不同类型的内部（员工）和外部用户提供单点登录 (SSO)、多因子认证和身份生命周期控制。

1.1 服务产品

客户可以从以下可用服务产品中选择，这些产品的事件容量均为每秒 400 个事件。

1.1.1 IBM Cloud Identity Connect

此云服务通过 ISAM 和 Open ID Connect (OIDC) 提供单点登录、面向基于云的 API 授权的认证、应用程序启动板、管理员报告和分析仪表板。此云服务使用基于现代化标准的认证和联合协议，将用户连接到应用程序（包括数百个常见应用程序的连接器）。此云服务与内部部署的 IBM Security Access Management (ISAM) 软件程序紧密集成，ISAM 作为支持软件，为客户提供解决方案，支持其业务线的内部应用和云端应用访问管理需求。

1.1.2 IBM Cloud Identity Connect for ISAM

此云服务与内部部署的 IBM Security Access Management (ISAM) 软件程序紧密集成，为客户提供解决方案，支持其业务线的内部应用和云端应用访问管理需求。此云服务要求客户具有针对 IBM Security Access Management (ISAM) 程序的活动的软件订购和支持 (S&S) 权利，并且 S&S 必须在客户的云服务订购期间保持活动状态。客户对此云服务的权利必须等同于客户的本地 ISAM 许可证权利。停止客户的 S&S 也将停止此云服务。此云服务不包含对 5.2 节中定义的支持软件的访问权限。

1.1.3 IBM Cloud Identity Essentials

此云服务为客户提供针对其当前使用的各种 IBM 应用和公共云应用的单点登录 (SSO) 功能。此云服务可配合 IBM MaaS360 使用，可提供额外的安全控制级别，比如条件访问。

1.1.4 IBM Cloud Identity Verify

此云服务为受 Cloud Identity Connect 保护的应用程序提供多因子认证或者通过直接 API 调用来提供此类认证，并为其他实施点（包括 RADIUS 客户机、Unix/Linux PAM 服务器和 Windows 服务器）提供此类认证，从而在访问数字服务时验证其身份。这包括诸如电子邮件、基于 SMS 和时间（软件令牌）的一次性密码、以及由 IBM Verify 提供技术支持的基于推送的移动生物识别认证等机制。此云服务与内部部署的 IBM Security Access Management (ISAM) 软件程序集成，为客户提供解决方案，支持其业务线的内部应用和云端应用访问管理需求。它可独立使用或者作为 Cloud Identity Connect、Cloud Identity Connect for ISAM 和 Cloud Identity Essentials 的补充来使用。

1.1.5 IBM Cloud Identity Govern

此云服务与内部部署的 IBM Governance and Intelligence (IGI) 软件程序紧密集成，ISAM 作为支持软件，为客户提供解决方案，支持其业务线的内部应用和云端应用访问管理需求。此云服务为组织提供云服务中的高级身份生命周期管理功能，并包含应用访问请求工作流程。

1.1.6 IBM Cloud Identity Connect and Verify

此云服务作为单一服务产品，为客户提供 IBM Cloud Identity Connect 和 IBM Cloud Identity Verify 的功能。

1.1.7 IBM Cloud Identity Connect Verify and Govern

此云服务作为单一服务产品，为客户提供 IBM Cloud Identity Connect、IBM Cloud Identity Verify 和 IBM Cloud Identity Govern 的功能。

1.2 可选服务

1.2.1 IBM Cloud Identity Non-Production

IBM Cloud Identity Non-Production Environment on Cloud 是一个单独的 IBM Cloud Identity Platform 实例，客户仅可将其用于内部非生产活动，包括但不限于测试、性能调优、故障诊断、内部基准评测、登台质量评估活动和/或使用发布的应用程序编程接口开发内部使用的云服务插件或扩展。此云服务可以选择包含可用性服务级别协议 (SLA)，但需遵守第 3 节“服务级别和技术支持”中的条款。该云服务每秒具有 100 个事件的容量。

1.2.2 IBM Cloud Identity Vanity Domain

虚拟域（一个域）允许客户使用客户组织拥有且与其更相关的域，而不是使用平台提供的现成缺省租户域。此域的 SSL 证书将由 IBM 进行维护并且将按年进行续订。

1.3 加速服务

1.3.1 IBM Cloud Identity Connect Solution Planning

该服务提供一 (1) 周的专业服务，期间 IBM 将执行以下部分或所有操作：

- 为基于云的 SaaS 应用程序建立单点登录
- 配置启动板以便于应用程序定位
- 使用现成的连接器连接应用程序
- 解决方案规划、架构和指导
- IBM 推荐方法和实践

1.3.2 IBM Cloud Identity Verify Workshop for Multi-Factor Authentication

该服务提供为期三 (3) 天的专业服务研讨会，重点讨论多因子认证挑战和使用 IBM Cloud Identify Verify 保护客户的应用程序。该研讨会将涵盖以下部分或全部内容：

- 将熟悉的认证嵌入到所有需要认证的数字交互和人员交互中
- 启用应用程序，使用开发者友好型 REST API 执行强认证
- 提供有关身份安全的行业最佳实践建议
- 精简的用户体验和使用方法，支持手机、平板电脑和笔记本电脑等所有设备

1.3.3 IBM Cloud Security Strategy and Planning

该服务提供为期三 (3) 周的专业服务研讨会，讨论如何应用云安全最佳实践，并重点关注基础架构和应用程序安全性。该研讨会将涵盖以下部分或全部内容：

- 为基于云的 SaaS 应用程序建立单点登录
- 配置启动板以便于应用程序定位
- 使用现成的连接器连接应用程序
- 解决方案规划、架构和指导
- 关于网络安全新趋势的洞察
- IBM 推荐方法和实践

1.3.4 IBM Cloud Identity Expert On Demand

该服务提供二十 (20) 小时的专业服务，在服务开始后三十 (30) 天内以每次两 (2) 小时会议的形式交付。该服务将安排一位 Cloud Identity 架构设计师来回答问题并提供指导和建议，但不限于：

- 技术技能，强化客户的 Cloud Identity 解决方案实施
- 有关客户 Cloud Identity 解决方案的架构和实施问题
- 有关客户 Cloud Identity 解决方案和/或策略的指导

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://www.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=735E5650E26711E69CCD7F0385C6524D

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 SaaS 支持概述 (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%	10%

* 订购费用是当月该索赔相关的合同价格。

3.1.1 关于此 SLA 的其他信息

在客户期限的前六十 (60) 天（“烧入周期”）期间，客户无权获得任何积分，因为 IBM Cloud Identity 环境未能实现本协议规定的最低 99.9% 的正常运行时间。如果在“烧入周期”之前或期间，IBM 发现现有客户配置、策略、数据或代码（“预先存在的组件”）意图迁移至 IBM Cloud Identity Service，而这样的操作会使 IBM Cloud Identity Service 无法成功实现本协议规定的正常运行时间百分比，IBM 将保留就此类“预先存在的组件”通知客户的权利并由 IBM 自定决定将这些组件从 SLA 配置中免除。如果 IBM 就任何免除的“预先存在的组件”通知客户，IBM 应负责尽可能向客户提供补救计划，以支持此类被免除组件达到本协议规定的正常运行时间百分比要求。除非经双方商定，否则客户应自行负责任何此类补救措施的成本。

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：

- 授权用户是有权通过任何方式和途径，直接或间接（例如，通过多路复用程序、设备或应用程序服务器）访问云服务的唯一用户。
- 员工是客户企业雇佣、付费或代表客户企业采取行动的个人，无论是否被授权访问云服务。
- “合格参与者”是指每个符合条件参与云服务所管理或跟踪的任何服务交付计划的个人或实体。
- 实例是对云服务的特定配置的每次访问。
- 互动是与云服务相关的专业或培训服务。

- 一起事件是指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。
  - 对于 Cloud Identity Connect，一起事件表示针对云服务的一个 HTTP 请求。
  - 对于 Cloud Identity Verify，一起事件表示通过云服务调用的任意多因子方法。

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 客户参考

客户同意 IBM 可在宣传或市场营销中将客户公开为云服务的订户。

5.2 支持软件

云服务包含以下支持软件：

下列支持软件只能与 IBM Cloud Identity Connect、IBM Cloud Identity Connect and Verify 和 IBM Cloud Identity Connect Verify and Govern Cloud Services 一起使用：

- IBM Security Access Manager Virtual Enterprise Edition

下列支持软件只能与 IBM Cloud Identity Govern 和 IBM Cloud Identity Connect Verify and Govern Cloud Services 一起使用：

- IBM Security Identity Governance and Intelligence Enterprise Edition
- IBM Security Identity Manager

5.3 MaxMind

此云服务包含由 MaxMind（可从 http://www.maxmind.com 获取）创建的 GeoLite2 数据。GeoLite2 可提供 IP 地理定位，以帮助通过 IP 地址来确定计算机的地理位置。

5.4 验证

客户将 i) 按照 IBM 及其独立审计员验证客户遵守协议的情况的合理所需，保存并根据请求提供记录和系统工具输出；并且 ii) 及时订购必需的权利并按照 IBM 当时的费率支付费用以及 IBM 在发票中指定的此类验证所确定的任何其他费用和责任。在云服务期限内以及本协议到期后的两年内，这些合规性验证义务均保持有效。