

# 在云中管理用户身份识别和访问

## 实行用户配置和访问控制，保护云部署环境中的用户和数据

### 目录

- 1 在云中以及跨云来平衡可扩展性、易用性和配置
- 2 实施联合单点登录，安全访问基于云的各种服务
- 3 针对基于云的用户实施全生命周期身份识别和访问管理
- 3 入门 – 评估云安全和隐私风险
- 4 为什么选择IBM?

能够与各部门、合作伙伴、客户和其他业务生态系统的组成部分共享服务和信息是云计算的一项主要优势。因此，成功的云部署依赖于安全有效地管理个人资源访问，以及保护数据避免丢失和损坏。从法律法规的角度而言，您必须能够控制、监控和报告谁正在访问哪些基于云的资源，以及目的何在。但管理数千乃至数百万个人ID是绝大部分IT部门所无法承受的。IBM能够帮助您解决这个问题。IBM解决方案可让客户联合并集中管理细粒度的访问策略，并在云中通过安全服务进行实施。除了提高云安全性，IBM解决方案还有助于降低管理成本，确保实现合规性以及加强整个业务环境的生产协作。

### 在云中以及跨云来平衡可扩展性、易用性和配置

谈到将关键工作负载和应用程序外包给云时，企业必须为适当的人员提供对这些工具的适当访问权限，以及他们开展自身工作或执行任务所需的必要信息。但在安全性和易用性之间取得适当的平衡可能相当具有挑战性。当数以百万计的用户需要访问基于云的资源时，用户配置（和取消配置）必须简便、有效并且可扩展。



自动身份识别和访问管理(IAM)解决方案可以应对这些挑战,并且同时包含云环境和传统的计算环境,这样您将不必管理两套凭据。借助IAM解决方案,您可以设置并执行策略,从而控制哪些人可以在哪些时间从哪些位置访问哪些信息,以及在设定的时间段内可以访问的信息量。一旦建立了凭据,授权用户可进行单点登录访问。您可以运用该解决方案随时重新确认所有权限,并在必要时迅速撤销权限。各种工具应当也可以监控、报告和主动预防策略违规。防止特权用户造成威胁尤其关键,因为内部用户可能会在有意或者无意地造成灾难性破坏。

面向云的IBM身份识别和访问管理解决方案可应对多个挑战并满足多种业务需求,包括:

- 广泛的用户基础,其中可能包括访问企业应用程序和第三方服务的员工、客户和合作伙伴
- 用户数量极其庞大(客户社区云访问可能涉及数百万用户)
- 适用于不同情况的不同需求和访问控制策略、敏感和非敏感数据(例如,访问未来产品设计与邀请客户参加即将举办的营销活动)
- 资源有限、预算紧张,不希望复制现有的IT安全基础设施直接用于云环境
- 全面的安全防护,满足各种法规遵从要求,帮助防止出现代价高昂且会损坏信誉的系统违规

## 实施联合单点登录,安全访问基于云的各种服务

在整个企业的业务生态环境中开展协作要求企业将自身的应用程序访问扩展至合作伙伴、客户和消费者。虽然身份识别和访问管理(IAM)实践可能十分完善并且在传统IT环境中能够实现自动化,但云还能将服务、应用程序和资源扩展到更广泛的用户群,其中可能包括来自受信任和不受信任的外部位置的员工、客户以及合作伙伴。企业需要能够将基于云的应用程序与内部应用程序紧密衔接在一起,从而让用户通过单点登录轻松地进行访问。联合身份管理提供了一种在云中以及传统计算基础设施内管理身份和访问的安全、可扩展的方式。

IBM联合身份管理解决方案可帮助简化云内外用户的生命周期管理和访问控制。IBM解决方案提供了基于策略的控制手段,可处理不同的用户配置文件,实现经过授权、审核以及身份验证的安全访问,无论云交付的应用程序和工作负载的连接位置和类型如何。通过提供一种联合方法,最终用户可以获得对这些应用程序的无缝登录体验,从而消除多用户ID和密码需求。联合方法还可以让企业更加有效地管理整个云基础设施的身份信息,同时保持用户数据的机密性。IBM解决方案基于SAML、Open ID和OAuth等开放标准,能够实现安全、灵活的业务协作。集成的密码自助服务功能可以让用户无需帮助台工作人员的帮助就能轻松在线重设密码。这有助于提高员工的工作效率,改善用户体验以及减少帮助台的呼叫数量,这些最终都能让您节省资金。

IBM身份识别和访问管理解决方案基于开放标准, 能够提供:

- 通过单一ID和密码单点登录访问多个基于Web的应用程序和云应用程序
- 用户身份创建和管理的自助服务(即密码重置)
- 用统一的方法管理传统以及基于云的用户和应用程序的身份与访问安全
- 跨各应用程序、数据源、操作系统甚至企业边界自动管理和实施访问控制策略
- 能够跟踪和记录用户活动、举报违规行为, 以及证实“职责分离”等策略的合规性
- 提供快速部署和实现价值的模块化基础, 从而随时间推移加强安全性

## 针对基于云的用户实施全生命周期身份识别和访问管理

企业需要对整个云环境中的用户、身份验证、访问、策略和配置进行集中的自动管理。这些功能有助于满足合规性需求、降低运营成本、加强安全状态以及提高运营效率。IBM软件用于在云管理中进行全生命周期身份管理, 保护和监控用户的资源访问以及提供合规性审计。功能包括:

- 对基于云的用户身份实行全生命周期身份管理(“从摇篮到坟墓”)
- 能够对基于云的管理员的特权身份(即系统和数据库管理员)进行监控、控制和报告

- 对云中的应用程序和数据实行访问和授权控制
- 实施基于角色的身份识别和访问管理, 让用户角色与其访问能力保持一致, 包括基于云的用户和应用程序
- 供最终用户对客户端/服务器应用程序进行桌面单点登录
- 对用户及其活动(包括云环境和传统环境)的合规报告和审计进行安全事故和事件管理

## 入门—评估云安全和隐私风险

IBM可帮助您根据既定的企业安全策略验证身份和访问实践, 从云中创造新的业务价值来源。云安全漏洞可能会对任务关键运营造成不利影响, 为用户和敏感数据带来风险。虽然安全漏洞并非云环境所独有, 但云计算的某些方面可能会为其自身带来挑战, 其中包括:

- 多租户 — 复杂的策略、治理, 以及对任务和数据访问需求存在很大不同的用户进行管理
- 虚拟环境 — 云是高度虚拟化的环境, 虚拟安全防护领域的发展相对不够成熟
- 高度灵活、快速的服务执行 — 损坏的虚拟映像可能在数十次供应之后, 其问题才能得到发现和纠正

IBM了解这些挑战，并且能够运用自身的综合战略、研究、服务、解决方案和经验帮助客户安全采用云计算。与IBM合作管理云计算身份和访问的优势包括：

- 降低风险
- 加强可视性与控制力
- 提高可扩展性和用户生产率
- 提升配置灵活性
- 加速审计过程

作为关键的第一步，IBM专家能够执行云安全评估，帮助您识别安全和隐私风险，并对当前安全状态与业内最佳实践和内部目标进行比较。由于对云安全控制、机制和架构具有深入的了解，IBM专业评估人员能够提供可行的建议，以便弥补安全漏洞并改进整体的云安全状态。

## 为什么选择IBM?

IBM采用云计算作为自身业务的重要组成部分，在安全举措方面开展了大规模的持续投资，并能够将自身的知识和整体方法应用到云安全防护方面，让客户能快速执行项目并获得投资回报。IBM深知身份识别和访问管理对于构建和维护可审计的安全云环境至关重要。让我们帮助您应对各种大型云用户社区所面临的挑战。我们的解决方案平衡了安全性和可用性，能够简化云计算环境中呈现的复杂用户配置文件和访问需求管理。

## 更多信息

如需进一步了解IBM Security，请联系您的IBM销售代表或IBM业务合作伙伴，或者访问：[ibm.com/security](http://ibm.com/security)

此外，IBM Global Financing 可帮助您以最经济高效和战略性的方式获得您的业务所需的 IT 解决方案。我们将与信用合格的客户展开合作，定制一个 IT 财务解决方案来满足您的业务目标，实现有效的现金管理，以及改善您的总体拥有成本。IBM Global Financing 是您投资关键 IT 投资和向前推进您业务的最智慧选择。有关更多信息，请访问：[ibm.com/financing](http://ibm.com/financing)



©版权所有 IBM Corporation 2011  
IBM Corporation Software Group Route 100  
Somers, NY 10589  
U.S.A.  
在中国印制  
2012年7月  
保留所有权利

IBM、IBM徽标和ibm.com是国际商业机器公司在美国和/或其他国家（地区）的商标。如果上述及其他IBM商标词汇在本文中第一次出现时标记了商标符号（®或TM），均代表在本文出版之际，它们是IBM在美国或其他国家注册的商标或普通法规定的商标。这些商标也可能是其他国家/地区的注册商标或普通法规定的商标。有关IBM商标的最新列表，请访问[ibm.com/legal/copytrade.shtml](http://ibm.com/legal/copytrade.shtml)的“Copyright and trademark information”部分。

其他公司、产品或服务名称可能是其他公司的商标或服务标记。

本文中对 IBM 产品或服务的引用不代表 IBM 打算在所有 IBM 运营的国家或地区都提供这些产品或服务。

我们已于发布之初对产品数据的准确性进行了审核。产品数据如有变更，恕不另行通知。IBM关于其计划、发展方向和意图的表述随时可能更改或收回，恕不另行通知，这些内容仅代表发展宗旨和目标。

IBM客户应自行确保遵守法律规定要求。请有能力的法律顾问提供有关任何相关法律的鉴定和解释的建议是客户自己的责任，它们可能会影响客户的业务以及客户为遵守这些法律可能需要采取的任何行动。IBM不提供法律建议，也不表示或保证其服务或产品将确保客户遵守任何法律。



请回收利用

WGE03016-CNZH-00