在云中管理用户身份和访问

用于保护云部署中用户和数据的用户配置和访问控制

目 录

云计算的一大优势就是能够与各部门、合作伙伴、客户和企业生态系统的其他组成部分共享服务和信息。因此，云部署成功与否取决于能否安全高效地管理个人对资源的访问并避免数据丢失或数据损坏。从法律法规角度而言，您必须有能力控制、监控和报告哪些人正在访问哪些基于云的资源及其访问目的。但是数千乃至数百万个个人标识的管理工作，让大多数 IT 部门都不堪重负。IBM 可以提供帮助。IBM 解决方案可帮助客户联合并集中管理细粒度的访问策略，在云中通过安全服务实施这些策略。除增强云安全性之外，IBM 解决方案还可以帮助降低管理成本、确保合规性，提高业务环境中的协作成效。

在云中和云之间实现可扩展性、易用性和配置的平衡

在将关键工作负载和应用外包至云方面，企业必须为适当人员提供要执行工作或任务所需工具和信息的适当访问权。但要在安全性和易用性之间寻求适当的平衡绝非易事。当数百万名用户需要访问基于云的资源时，用户配置（和取消配置）必须简单、高效且可扩展。

自动化的身份和访问管理 (IAM) 解决方案可以解决这些难题，并且包含云环境和传统计算环境，因此，您不必管理两套凭证。通过 IAM 解决方案，您可以设置并实施策略，确定哪些人可以在何时从何地访问哪些信息，以及在设定的时间段内可以访问的信息量。一旦确立凭证之后，经过授权的用户就将具有单点登录访问权。一段时间之后，您可以使用此解决方案来重新确认所有授权，并根据需要立即撤销这些授权。另外，还应提供一些工具来监控、报告和主动预防策略违规。防范特权用户威胁尤为关键，因为无论是有意还是无意，内部人员都可能导致灾难性的破坏。

IBM 面向云的身份和访问管理解决方案可以应对各种挑战和业务需求，包括：

- 广泛的用户群，包括访问企业应用和第三方服务的员工、客户与合作伙伴
- 数量庞大的用户（面向客户社区的云访问可能涉及数百万的用户）
- 应用于不同环境以及敏感数据和非敏感数据的各种需求和访问控制（例如，旨在获取未来产品设计的采购访问权与邀请客户参加即将举办的市场活动）
- 有限的资源、紧缩的预算和不希望只是为云复制现有 IT 安全基础架构的要求
- 全面的安全措施，满足法规合规性要求，并帮助预防高成本的、有损声誉的系统违规

实施联合单点登录，安全访问基于云的服务

要在组织的业务生态系统中通力协作，企业就必须将其应用访问权扩大至合作伙伴、客户与消费者群体。虽然在传统 IT 环境中可能已经确立并且自动执行了身份和访问管理 (IAM) 实践，但是云可以将服务、应用和资源扩大至更广泛的用户群，包括来自可信和不可信外部位置的员工、客户和合作伙伴。各组织需要能够将基于云的应用与内部应用捆绑在一起，便于用户通过单点登录轻松访问这些应用。联合身份管理提供了一种安全且可扩展的方法，用于在云中和传统计算基础架构内管理身份和访问权。

IBM 联合身份管理解决方案可帮助简化生命周期管理和对云中内部及外部用户的访问控制。IBM 解决方案提供基于策略的控制方法，可处理不同的用户个人档案，并支持安全、经授权、经审计且经认证的访问，而不论是从什么地点以何种方式连接到利用云交付的应用和工作负载。通过提供联合方式，最终用户能够无缝登录至这些应用，而不必提供多个用户标识和密码。联合方式还支持企业更高效地管理云基础架构中的各种身份，同时保持用户数据的机密性。基于诸如 SAML、Open ID 和 OAuth 等开放式标准，IBM 解决方案支持安全而灵活的业务协作。集成的密码自助式功能支持用户轻松在线重置自己的密码，而无须帮助中心人员的帮助。这有助于提高员工工作效率、增强用户体验并减少帮助中心来电数量，最终节省了成本。

IBM 身份和访问管理解决方案基于开放式标准，可提供以下功能：

- 单点登录，通过单一的标识和密码访问多个基于 Web 的应用和云应用
- 用户自助服务，用于身份创建和管理（即，密码重置）
- 为传统和基于云的用户及应用提供一致的身份和访问安全性管理方法
- 跨所有应用、数据源、操作系统甚至是公司界限，自动管理和实施访问控制策略
- 跟踪和记录用户活动、报告违规行为，并证明符合各种策略，例如“职责分离”策略
- 为快速部署和快速实现价值奠定模块化的基础，随着时间推移，可通过增加其他安全措施来加以强化

为基于云的用户获取完整的生命周期身份和访问管理

企业需要在云中和云之间以自动化方式集中管理用户、认证、访问、策略和配置。这些功能有助于满足合规性需求、降低运营成本、增强安全态势，并提高运营效率。面向云中的完整生命周期身份管理的 IBM 软件可以管理、保护和监控用户对资源的访问，并提供合规性审计。这些功能包括：

- 对基于云的用户身份的完整生命周期身份管理（“从创建到注销”）
- 为基于云的管理员监控、控制和报告特权身份（即，系统和数据库管理员）
- 对云中的应用和数据的访问和授权控制
- 基于角色的身份和访问管理，使用户角色与其访问功能保持一致，包括基于云的用户和应用
- 最终用户能够以桌面单点登录方式登录至客户机/服务器应用
- 安全事故和事件管理，用于云环境和传统环境中用户及其活动的合规性报告与审计

入门 - 评估云安全性和隐私风险

IBM 可以根据已确立的企业安全策略来验证身份和访问实践，帮助您通过云创造新的商业价值来源。云安全损害会对业务关键型运营造成负面影响，使用户和敏感数据暴露于风险之中。虽然安全漏洞并不是云环境所特有的现象，但是云计算的某些特征可能会使它们更加难以处理，这些特征包括：

- 多租户 - 使策略、治理和用户管理能力更加复杂，这些用户需要执行各种不同的任务，具有不同的数据访问需求
- 虚拟环境 - 云是高度虚拟化的环境，虚拟安全性是一个相对不成熟的领域
- 弹性高、服务执行迅速 - 虚拟映像一旦损害，就可能需要数十次配置才能发现和纠正问题

IBM 了解这些挑战，并且应用其全面的战略、研究、服务、解决方案和经验来帮助客户以安全的方式接纳云计算。与 IBM 协作管理云中的身份和访问具有的优势包括：

- 风险更低
- 可视性和可控性得到增强
- 可扩展性和用户效率更高
- 配置更灵活
- 审计流程更快完成

关键的第一步是，IBM 专家可以执行云安全评估，帮助发现安全和隐私风险，并将当前安全状态与行业最佳实践和内部目标进行比较。通过对云安全控制、机制和架构的深入了解，IBM 评估专家可以提供切实可行的建议，用于弥补安全漏洞，改善云的整体安全态势。

为何选择 IBM？

IBM 已在自身业务的重要部分中采用了云计算，持续对安全计划投入了大量资金，能够将其掌握的云安全知识和整体性方法传授给客户，快速执行，并快速实现投资回报。IBM 知道，身份和访问管理对于构建和维护安全且可审计的云至关重要。请让我们帮助您解决各种大型云用户社区所存在的挑战。我们的解决方案可以实现安全性与易用性的平衡，可简化云计算环境中存在的复杂用户个人档案和访问需求的管理过程。

更多信息

要了解有关 IBM Security 的更多信息，请与您的 IBM 销售代表或 IBM 业务合作伙伴联系，或者访问以下 Web 站点：ibm.com/security

此外，IBM 全球融资部可帮助您以最经济实惠的战略方式获取企业所需的 IT 解决方案。我们将与信誉良好的客户协作定制 IT 融资解决方案，帮助您实现业务目标、有效管理现金并降低总体拥有成本。IBM 全球融资部是您为关键 IT 投资融资并推动业务发展的最明智的选择。有关更多信息，请访问：ibm.com/financing

IBM Corporation
Software Group
Route 100
Somers, NY 10589
U.S.A.

美国印刷
2011 年 12 月

WGE03016-CNZH-00