Microsoft

使用 Azure Active Directory
管理和保护对应用程序的访问

第 1 节

什么是身份和访问管理?

什么是身份和访问管理?

数字化转型

云计算和移动设备已经改变了现代工作场所。全球范围内的劳动力都逐渐具备了灵活性，他们可以使用免费和低成本的软件即服务 (SaaS) 应用程序在任何地方工作，解决生产力和协作难题。很多大型企业正在将应用程序和计算迁移到云中以实现其体系结构的现代化，各行各业也在利用新的云服务来生成满足其特定需求的自定义应用程序。企业从这场新技术的浪潮中获得了更高的生产率，但数字化转型也带来了三个新的挑战。

什么是身份和访问管理?

新的挑战

安全风险：在这场“云革命”之前，IT 是技术上的守关人。你管理和保护的应用程序和平台都包含在网络范围内，并且登录到贵公司资源中的每个人都需先通过防火墙的验证。而这种情况已经不复存在了。你的员工对他们所使用的技术拥有了更强的控制力，其中大部分是通过 Internet 实现的。网络攻击者已学会利用这些漏洞。即使用户知道帐户的正确密码，你也无法完全确定他们就是帐户的主人。

管理负担：终结点的激增为用户提供了更多的连接方式，但也为管理工作带了巨大的负担。很多企业都不了解员工使用的所有工具（即使有明确的清单），大量的云应用也需要企业管理多种身份系统，这样既提升了成本，也加剧了现有的安全风险。

糟糕的用户体验：用户也觉得很痛苦。他们享受新技术所带来的灵活性，但也需要记住更多的凭据，这让他们很烦恼。

安全风险

管理负担

糟糕的用户体验

什么是身份和访问管理?

将身份和访问管理作为中心控制平面

上述难题的共同点在于身份验证系统的效率低下。身份已取代网络边界成为新的控制平面。你需要能够在整个企业中连接不同工具、体系结构、设备和服务的解决方案，从而更好地保护组织以及管理员工和外部合作伙伴的访问。身份和访问管理 (IAM) 系统可将访问统一在一个系统下，为你提供更强的控制力。它们提供跨组织边界的无缝协作，同时提高公司资源的安全性。若采用出色的 IAM 解决方案，可通过一组凭据将用户连接到其所有工作应用程序（无论是在云中还是在本地）。IAM 解决方案旨在让用户只访问他们需要的资源，并阻止未经授权的用户访问其不应访问的数据。你可在一个集中式的门户中管理用户访问权限，从而减少了预配和取消预配用户帐户过程中的许多手动操作。IAM 解决方案还提供跨身份和应用管理安全策略的工具。更佳的 IAM 解决方案可以更好地保护身份、改善用户体验并提高管理效率。

IAM 解决方案
可以解决这些难题

更好地保护身份

改善用户体验

提高管理效率

第 2 节

Azure AD 概述

Azure AD 概述

一款全面的解决方案

Microsoft Azure Active Directory (Azure AD) 是云中一个全面的 IAM 解决方案，在管理目录、应用程序访问和高级身份保护方面处于市场领导地位。使用 Azure AD，组织能管理并保护员工、合作伙伴和客户用于访问所需应用和服务的身份。Azure AD 帮助数百万组织管理和保护超过十亿个身份。

访问现代化

管理并保护对组织本地和云中的数据和资源的访问。将所有用户、应用程序和设备连接到云，从而实现无缝且安全的访问以及更强的可见性和控制力。自动执行工作流并启用自助服务选项，有助于降低成本和提高用户工作效率。

保护和管控

用户的凭据信息每天都会遭受大量攻击，应对方法是在尽可能广泛的信号范围内持续跟踪正常和异常行为、采用人工智能并实现自动化响应。通过及时访问正确的资源、定期审查访问情况并强制执行策略，实现工作效率和安全性的平衡。

联系和协作

借助可靠的云服务扩展业务，该服务可通过行业领先的安全性和灵活性扩展到数百万个用户。通过友好易用的自助服务体验和内置安全控件，与外部用户建立联系并提高他们的工作效率。

开发和集成

生成能让用户轻松地使用其 Microsoft 个人、工作或学校帐户或者社交帐户登录的应用程序。开始连接到 Microsoft Graph（Microsoft 365 中的数据及智能网关），并生成功能丰富的应用程序。启用单一登录、自动执行用户预配并与全世界最大的组织建立联系。

第 3 节

适用于应用程序的 Azure AD

适用于应用程序的 Azure AD

一款通用平台

使用 Azure AD，可以为混合基础结构中的每个用户管理一个通用身份，让他们访问所需的所有应用程序，包括云和本地业务线应用程序。在通用平台中管理所有身份，提高管理效率并获得更强的控制力。将精细安全策略应用于组织中使用的每个应用程序。

适用于应用程序的 Azure AD

节省时间和费用

Azure AD 已预先集成数千种应用程序，其中包括很多热门的应用程序（如 Workday、ServiceNow、SuccessFactors、Adobe 和 Concur），使你可更轻松地将这些应用提供给用户。使用一个控制台，部署一致的策略并监视访问权限。通过自助服务帐户管理，可实现用户预配和生命周期管理工作流的自动化，并节省时间和资源。你还可从 HR 工具中导入用户信息作为可信来源，使得在管理用户属性时无需自定义脚本或手动流程。

通过 Azure AD 配置的应用启用了单一登录 (SSO) 以实现无缝访问，这意味着用户不必记住每个应用帐户的凭据，也不必重用弱密码，避免数据泄露。已配置进行自动预配的帐户使用户能够尽快地访问新资源。在入站预配方面，Azure AD 确保新员工在第一天就可以访问所有相关的资源。

节省时间和费用

内置 SaaS 集成

单一登录

新用户可在首日进行访问

适用于应用程序的 Azure AD

提供对所有应用的更安全的访问

Azure AD 跨所有应用（包括 SaaS 应用和本地业务线应用）为你提供全面的身份保护。无论用户是请求访问 Microsoft Word 还是 Box，Azure AD 都会在授予访问权限之前确认用户的身份。你还可以制定访问管理策略，确保用户只有在需要时才可以访问他们需要的内容。你可以要求用户请求访问权限，还可以设置用户可以访问应用程序的时间限制，并定期对访问情况进行合规性审查。

Azure AD 还利用 Microsoft Intelligent Security Graph 和机器学习的功能，分析我们所有产品和服务中的数万亿个信号，从而发现异常行为并为每个会话分配相对风险。Azure AD 查看设备、位置以及其他上下文信息以评估登录风险。你可以制定自动应用安全措施的 Azure AD 条件访问策略，例如在认为登录存在风险或满足特定策略条件时阻止访问请求或要求重置密码。

应用程序安全措施

身份保护

访问管理

条件访问策略

第 4 节

如何使用 Azure AD 管理和保护应用

Azure AD 利用自动化、自助服务和策略实施，使保持控制力和降低成本变得简单。

如何使用 Azure AD 管理和保护应用

Azure AD 应用集成

通过 Azure AD 应用程序库，可轻松地配置数千个预集成应用中的任何一个，并将其连接到你的租户。这些应用均支持 SSO 体验，并且可轻松地在每个应用的基础上或针对企业级策略配置应用的 Azure AD 条件访问。添加应用并根据需要对其进行配置后，被授予访问权限的用户可以在Azure AD"我的应用"门户（此处是最终用户发现和启动应用的集中式门户）中轻松找到它。

如果你已为组织生成了一个应用或需要为组织集成一个应用，则还可以请求将其列在 Azure AD 应用程序库中。

探索数千个预先集成的应用 >

安全混合访问

使用 Azure AD 应用程序代理，可提供对基于声明的本地 Web 应用程序的安全、远程访问，且无需使用 VPN。应用代理需要安装一个轻型连接器，并提供与通过 Azure AD 应用程序库连接的 SaaS 应用相同的 IT 和最终用户体验。

或者，若你想利用现有的基础设施投资（例如与 F5 ZScaler、SAP、Oracle 或 Ping Identity 等合作伙伴合作）以连接其他类型的应用（例如使用基于标头或 Kerberos 身份验证协议的应用程序），也可以这样做，且仍然可获得 Azure AD 的集中化和安全方面的优势。

阅读了解如何通过应用代理添加本地应用程序 >

连接其他合作伙伴应用网络和云 >

如何使用 Azure AD 管理和保护应用

自动化预配

通过 Azure AD，可在热门的 SaaS 应用程序中实现用户身份的创建、维护和删除自动化。当新人员加入团队或组织时，你可在正确的系统中自动为他们创建新帐户。你可以针对人员离开团队或组织的情况设置策略，从而自动从正确的系统中停用其帐户。通过自动执行这些任务，可确保应用和系统中的身份根据目录或人力资源系统的变更保持最新，从而减少错误并节约时间。

详细了解如何设置对 SaaS 应用的自动预配和取消预配 >

组管理

通过向单个用户或整个 Azure AD 组提供访问权限，Azure AD 帮助你授予对组织资源的访问权限。若使用组，资源所有者可为组中的所有成员设置访问权限，而不必向各个成员一一授予权限。这是一种更安全的方法，因为你意外授予某位成员不恰当访问权限的可能性较小，同时还可以节约时间。你也可通过基于身份属性的策略使注册自动化，从而动态地扩展组管理。

了解如何在 Azure 门户中创建组 >

如何使用 Azure AD 管理和保护应用

用户自助服务

某些任务不需要 IT 专业人员完成，而你可通过 Azure AD 将这些任务委托给组织中的其他人。你可以对用户进行授权，让用户能在 Azure AD 中创建和管理自己的安全组。组所有者可以批准或拒绝成员身份请求，也可以委托他人控制组成员身份。

设置自我托管组 >

自助服务也扩展到用户。如果用户拥有经过验证的电子邮件，他们可通过自助服务门户注册帐户，还可以使用该门户重置密码。这样为服务台节省了大量时间和费用。

配置自助服务密码重置 >

身份验证现代化

如果当前使用的是本地身份验证，例如 Active Directory 联合身份验证服务 (AD FS)，则你可考虑将应用迁移到 Azure AD。你保有同样的用户权益（例如 SSO），还从云中获得了可伸缩性和安全性方面的优势，例如使用 Azure AD 条件访问对各个应用进行精细的访问控制，或通过 Azure AD B2B 协作向合作伙伴授予对资源的访问权限。使用 SAML 2.0、WS 联合身份验证、OAuth、OpenID Connect 标准进行联合登录的应用都可以迁移。

制定 Azure AD 条件访问策略，保护对应用的访问 >

使用 Azure AD B2B 与外部合作伙伴无缝协作 >

将任何云或服务器上的任何应
用安全地连接到 Azure AD。

已连接 1 百万个活跃且独特的应用。

Microsoft

立即开始使用。

开始为期一个月的 Azure AD 免费试用，体验它的强大功能，
助你轻松地管理用户对所有应用的访问并保护企业。