Tivoli software

IBM

解决组织内外及组织之间的单点登录

白皮书

2009年3月

目录

2 概述

4 IBM Tivoli Unified Single Sign-On: 全面解决SSO问题

5 IBM Tivoli Access Manager for Enterprise Single Sign-On

7 IBM Tivoli Access Manager for e-business

9 IBM Tivoli Federated Identity Manager

10 结束语

11 更多信息

11 关于IBM Tivoli软件

概述

随着安全威胁愈加复杂、信息安全法规不断增多，组织在对访问敏感数据的控制方面受到的压力不断增大。许多组织的基础设施一直在不断扩展和演化，这导致了多样的硬件和软件组合，还有同样多样的安全标准和登录过程。与此同时，为支持新业务计划，如今IT必须支持3种访问途径:

- 组织内的应用程序。这些是企业单点访问应用程序，包含对Microsoft® Windows®、Web、Java™、Citrix、Microsoft Windows Terminal Services和大型机应用程序的访问。
- 公司Web应用程序，可保护通过Web访问的信息和资源。这些是Web应用程序，包含Web服务器、Web应用程序和门户——所有这些都处于单个域中。
- 以一种安全可信的方式从其他合作伙伴、或在组织中不同业务线之间无缝地访问资源的联邦应用程序。这些是跨域应用程序，包含Web服务器、Web应用程序和门户，涉及跨域交换。联邦是一种高效的方式，可连接业务生态系统中的合作伙伴和供应商，从而快速应用新采购的资产，或协调组织中的不同部门(这些部门可能拥有不同的安全措施)。

IBM Tivoli Unified Single Sign-On全面涵盖了单点登录(SSO)配置和需求

IBM Tivoli® Unified Single Sign-On解决了全部三种访问需求，而且支持异构环境。IBM Tivoli Unified Single Sign-On全面涵盖了单点登录(SSO)配置和需求，能帮助组织完全实现对端到端单点登录的承诺。

IBM Tivoli Unified Single Sign-On的益处包括:

- 解决组织对企业单点登录、Web单点登录和联邦单点登录的要求。
- 消除对记忆和管理用户名及密码的需要，使登录和访问自动化，简化最终用户体验。
- 借助对整个Java、Microsoft .NET和大型机环境内的异构Web应用程序和服务的集中身份验证、访问和单点登录，提高可见性和遵从性。
- 使用多种形式的凭证简化应用程序整合，并促进在企业内跨越可信的业务合作伙伴和部门共享更多安全信息。
- 减少不良的最终用户密码行为，通过广泛、强大的身份验证机制和访问控制，增强安全性。
- 通过减少密码重设呼叫的数量，降低与密码相关的帮助台成本。
- 支持全面的自助服务会话管理，提高安全性和用户效率。

IBM Tivoli Unified Single Sign-On由三种行业领先的单点登录产品组成:

- IBM Tivoli Access Manager for Enterprise Single Sign-On
- IBM Tivoli Federated Identity Manager
- IBM Tivoli Access Manager for e-business

本白皮书分析了这三种产品各自的单点登录功能，以及这些解决方案在合作提供统一的单点登录时的强大功能。

Tivoli Unified Single Sign-On组合了3种行业领先的单点登录产品，可全面解决3种SSO请求来源: Internet、外部网和内部网/自助终端。

IBM Tivoli Unified Single Sign-On: 全面解决SSO问题

为说明Tivoli Unified Single Sign-On如何全面解决单点登录，让我们看一下作为SSO请求来源的三个示例环境: Internet，外部网(机场休息室或上网中心，您在其中通过Web访问应用程序)，以及内部网/自助终端。

IBM Tivoli Access Manager for Enterprise Single Sign-On适用于企业，适用于安装了IBM Tivoli Access Manager for Enterprise Single Sign-On客户机代码的客户机发出请求的任何情况。IBM Tivoli Access Manager for e-business解决Web目标，适用于全部三种输入请求的可能来源: Internet、外部网和内部网。对于多域或跨域配置，IBM Tivoli Federated Identity Manager与IBM Tivoli Access Manager for e-business配合使用，可在整个Internet、外部网和内部网范围内处理访问请求。

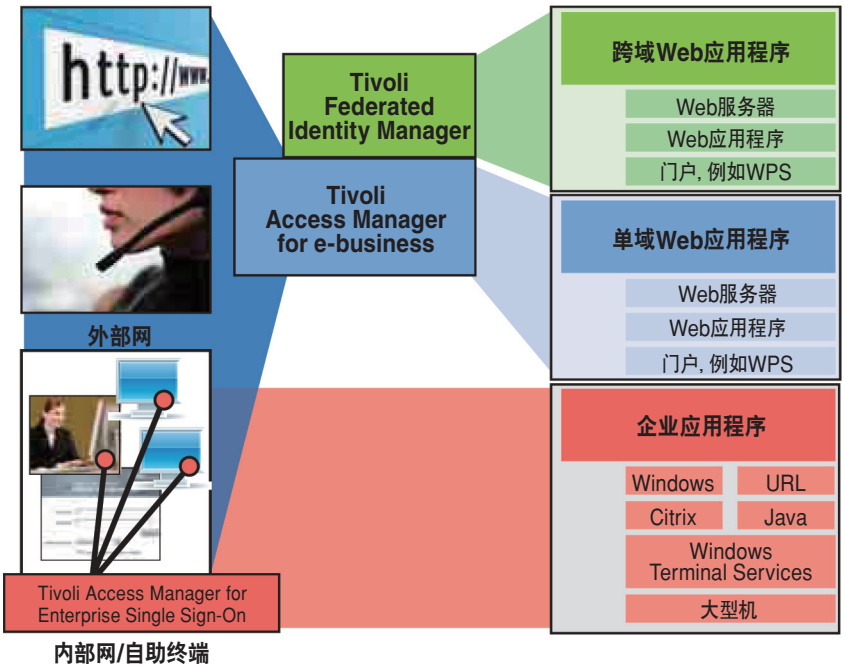

图1: Tivoli Unified Single Sign-On全面解决您的单点登录需求

Tivoli Access Manager for Enterprise Single Sign-On为企业内应用程序提供全面的单点登录。

IBM Tivoli Access Manager for Enterprise Single Sign-On

Tivoli Access Manager for Enterprise Single Sign-On使企业能够自动访问公司信息、增强安全性，并在企业端点加强遵从性。Tivoli Access Manager for Enterprise Single Sign-On解决全面的单点登录可能情况，包括Microsoft Windows、Web、Java、Citrix、Microsoft Windows Terminal Services和大型机应用程序。一般而言，IBM Tivoli Access Manager for Enterprise Single Sign-On是一种解决方案，应用于可在客户机上安装代码的环境(例如公司台式机、自助终端、Citrix环境或Microsoft Terminal Services环境)。

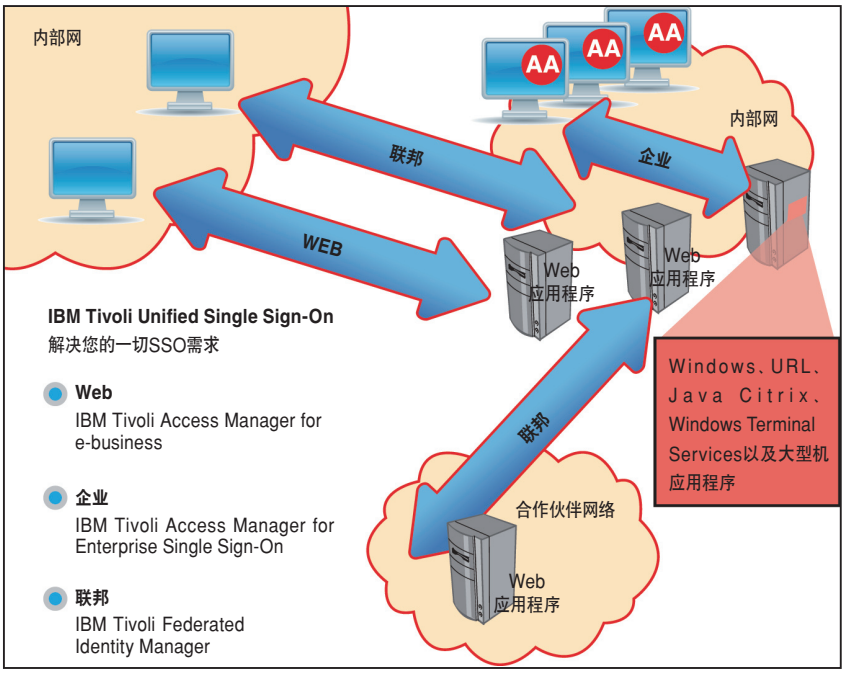

图2: Tivoli Unified Single Sign-On为您的业务可能涉及的全部三个流程交付自动化登录

在图2中，IBM Tivoli Access Manager for Enterprise Single Sign-On的AccessAgent(访问代理，用红圈中的"AA"符号表示)为多种企业应用程序(包括Tivoli Access Manager for e-business)提供单点登录。AccessAgent代码安装在每台利用此SSO功能的客户机上，并配合IBM Tivoli Access Manager for Enterprise Single Sign-On IMS™ Server使用，后者管理凭证、策略、审计日志和备份。

Tivoli Access Manager for Enterprise Single Sign-On提供了以下功能，无需改变现有IT基础设施:

- 面向所有用户组的强大身份验证
- 具有工作流自动化的企业单点登录
- 全面的会话管理
- 用于编写审计和遵从性报告的以用户为中心的访问追踪
- 轻松且更安全的远程访问——随时随地进行
- 与用户配置技术相整合

IBM Tivoli Access Manager for Enterprise Single Sign-On能帮助企业更有效地管理业务风险、满足法规遵从性、降低IT成本和提高用户效率。借助IBM Tivoli Access Manager for Enterprise Single Sign-On，企业在强大的安全性和便利性方面一举两得。

Tivoli Access Manager for e-business为公司Web应用程序提供单点访问，保护通过Web访问的信息和资源。

IBM Tivoli Access Manager for e-business

Tivoli Access Manager for e-business是面向公司Web应用程序的身份验证和授权解决方案，允许您交付Web单点登录，并控制用户对通过Web访问的受保护信息和资源的访问。通过提供一种集中、灵活且可伸缩的Web SSO和访问控制解决方案，IBM Tivoli Access Manager for e-business允许您构建高度安全且易于管理的基于Web的应用程序和电子商务基础设施。您能结合基于Internet的标准应用程序来使用Tivoli Access Manager for e-business，以实现对内部网上的应用程序和数据的高度安全并可良好管理的访问。访问可来自内部网、Internet或外部网。

如图2所示，IBM Tivoli Access Manager for e-business期望所收到的基于Web的请求来自一个客户机，其主要任务是验证用户、允许其访问有权限的资源、管理用户会话以及在整段会话期间为该用户提供Web单点登录。对于不需安装软件而仅能使用浏览器的Internet、内部网或外部网应用程序而言，这是最合适的。

Tivoli Access Manager for e-business能整合到现有的或新兴的基础设施中，提供集中化的策略管理功能。Tivoli Access Manager for e-business与IBM WebSphere® Application Server、IBM WebSphere Portal、IBM Tivoli Identity Manager、IBM Tivoli Access Manager for Enterprise Single Sign-On和IBM Tivoli Federated Identity Manager相整合，构成了完整的企业身份管理解决方案。

许多企业不仅使用IBM Tivoli Access Manager for e-business处理来自Internet的Web请求，还将Tivoli Access Manager for e-business部署到其内部网环境或私有网络中，以管理员工和承包人对Web资源的访问。IBM Tivoli Access Manager for Enterprise Single Sign-On与IBM Tivoli Access Manager for e-business整合，自动地提供登录IBM Tivoli Access Manager for e-business所需的身份和密码。在此配置中，IBM Tivoli Access Manager for Enterprise Single Sign-On处理所有应用程序登录，包括向Tivoli Access Manager for e-business的登录，而Tivoli Access Manager for e-business无缝地登录进它管理的Web资源。

Tivoli Federated Identity Manager支持全部3种主要联邦标准，从而为联邦单点登录提供了最高的灵活性。

IBM Tivoli Federated Identity Manager

联邦是指两个或更多可信的业务合作伙伴组成的团体，其遵照的业务和技术协议允许来自联邦合作伙伴(成员公司)的用户以一种安全可靠的方式，无缝地访问另一家合作伙伴的资源。在联邦业务模型中(其中，服务是联邦化的，或可以与业务合作伙伴共享)，根据有关实体间达成的协议，一家公司的用户的身份将被转换，以合法访问另一家公司的Web站点，而另一家公司无需了解该用户的原始身份。Tivoli Federated Identity Manager的这种身份转换功能使合作伙伴组织能够制定关于另一家公司用户(例如客户、供应商或客户机员工)的访问和授权决策，而无需为该第三方用户创建和管理身份数据。

使用Tivoli Federated Identity Manager，用户只需获知和使用唯一一组用户ID及密码，就可访问其域中的Web站点和其他公司域中的Web站点。这种方法扩展了单一登录，使其可包含涉及对多个域的访问的会话，此方法还简化了供应商、业务合作伙伴和客户之间的整合、通信和信息交换。

借助Tivoli Federated Identity Manager，组织在配置与合作伙伴的跨域关系方面拥有最高的灵活性，因为此产品支持全部3种主要联邦标准: Liberty、WS-Federation和安全断言标记语言(SAML)，还支持新兴的以用户为中心的SSO框架，例如OpenID和CardSpace。由于Tivoli Federated Identity Manager与它所交互的应用程序是松耦合的，所以比起在每个应用程序中使用专有API来处理身份转换的其他方案，这些应用程序的部署会更快速，维护会更便宜。

Tivoli Unified Single Sign-On全面解决组织内外及组织之间的一切单点登录需求。

在图2所示情况下, Tivoli Federated Identity Manager使对其他合作伙伴系统的访问联邦化。实际上, 这扩展了Tivoli Access Manager for e-business所管理的单域情况, 而且在Tivoli Access Manager for e-business和Tivoli Federated Identity Manager的合作下, 多域(联邦) Web事务能够以一种安全、经过验证且可审计的方式发生。

结束语

Tivoli Unified Single Sign-On全面解决组织内外及组织之间的一切单点登录需求。Tivoli Unified Single Sign-On还与其他IBM身份和访问管理解决方案相整合, 提供完整的端到端身份、访问和安全遵从性解决方案。与Tivoli Identity Manager的整合有助于确保用户能被集中管理, 使单点登录在所有使用情况下获得全面支持。

IBM为企业安全提供了统一的策略, 允许您在安全堆栈的任意位置开始应用, 再逐步推行到整个安全领域, 同时, IBM解决方案的广度和整合的深度可满足不断增长的需求。Tivoli Unified Single Sign-On是这个统一策略的一个出色例子。企业应当考虑自身的统一单点登录需求并进行投资, 以获得从开始就解决端到端单点登录需求的解决方案, 或获得能够按需与企业一同成长的解决方案。来自多家供应商的单点解决方案无法提供相同的广度和整合功能。

IBM使您能够集中精力, 在整个IT安全风险领域内, 通过灵活且适应性强的方法, 降低保证企业安全的复杂性, 从而驱动业务创新。IBM可掌控全局, 包括身份和访问控制、威胁防范、托管服务、大型机安全、信息和数据安全以及服务管理。IBM随时支持您的长期安全目标, 拥有解决更广泛的安全管理需求所需的广度和深度。

更多信息

如需了解有关IBM Tivoli Unified Single Sign-On的更多信息，请联系您的IBM销售代表或IBM业务合作伙伴，或者访问**ibm.com**/tivoli

关于IBM Tivoli软件

Tivoli软件为组织提供了一个服务管理平台，通过提供可视化、可控化和自动化，交付优质服务——可视化可用于查看和理解业务运转；可控化可用于有效管理业务，以帮助尽可能地降低风险、保护品牌；自动化有助于优化业务，降低运营成本，更快地交付新服务。与以IT为中心的服务管理不同，Tivoli软件提供了一个用于管理、整合和调整业务和技术需求的通用基础。Tivoli软件旨在迅速满足组织最急迫的服务管理要求，帮助主动响应不断变化的业务需求。Tivoli软件组合以世界级的IBM服务、IBM支持和活跃的IBM业务合作伙伴生态系统为后盾。Tivoli客户和业务合作伙伴还能够通过参与遍及全球、独立运作的IBM Tivoli用户组来利用彼此的最佳实践——请访问: www.tivoli-ug.org

此外，IBM Global Financing能根据您独特的IT需求定制财务解决方案。如需了解有关优惠信息、灵活的支付方案和贷款、资产回购和转让的更多信息，请访问: **ibm.com**/financing

客户自行保证遵守法律法规要求。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、审计和会计建议，也不代表或保证其服务或产品能保证客户遵守法律或法规。

本出版物中对IBM产品和服务的引用不代表它们可用于所有IBM运营的国家。

到发布之日止，产品数据都进行了准确性审校。产品数据可能随时更改，恕不通知。关于IBM未来方向或打算的声明仅代表IBM的发展目标，如有变更，恕不另行通知。

本文档中的信息按 "原样" 提供，不承担任何隐含或明确的担保。IBM明确表示对于适销性、适合于特定用途的适用性或不侵权性不做任何保证。IBM产品的担保依据是其遵循的协议(例如IBM Customer Agreement、Statement of Limited Warranty、International Program License Agreement等)中的条款和条件。