IBM 软件
思想领袖白皮书

2011 年 1 月

如果数百万人需要访问：日益互联的世界中的身份管理

可进行伸缩以满足如今大量用户的最佳实践解决方案

IBM

目录

简介

如今客户、业务合作伙伴、供应商和您所有的其他人员都有一个想法。他们想参与。他们希望访问您的网络或您的云计算进行采购，查找信息或使用应用程序。他们的数目有好几千，很多时候有数百万。

他们的兴趣和参与可对企业有利。但是您如何管理如此庞大的人群呢？身份管理的手动流程，包括从授权访问资产到管理用户账户，是无法进行伸缩的流程的典型示例。当用户数量较少时，这种流程可以发挥作用。但是如果用户数达到好几千时，手动步骤就成为一个很大的负担，如果用户数达到数百万时，手动流程就根本不可行了。试想一下重置密码。您怎样才能使咨询台大到足够应对遍及全球的客户？

随着组织通过向大量的内部和外部在线用户（其中许多用户都是移动的）开放自己的系统来转换业务，组织越来越多地采用自动化解决方案，这些解决方案可以保护敏感数据，支持最终用户自助服务并帮助解决问题。在现在物联化、互联化和智能化的 IT 运营中，身份管理最佳实践可以有助于确保满足智慧地球访问需求所需的安全、优化且符合法规的操作。

基于自助和访问控制的有效管理

现在对有效的身份管理的需求是互联化爆炸式增长的结果。例如，保险公司直到最近才管理数千名员工的访问，现在却需要管理数百万通过销售门户进行在线交易的客户和合作伙伴。

以前只管理其员工访问的政府机构现在需要管理数百万公民的访问以及其他在线访问信息的广泛的机构。医疗保健、金融和其他客户服务行业等领域的组织在很大程度上依赖于许多合作伙伴和消费者之间的互动和数据交换。

结果，在线业务运营的范围和需求出现前所未有的突然性增长，对组织的身份管理系统的需求也增加了。组织现在需要能够为员工、业务合作伙伴和外部最终用户提供所需的自助功能的系统，以便他们快速注册新的服务并解决个别问题（包括始终存在的密码重置问题），而无需联系咨询台。同时，组织需要为包括 IT 管理员、业务经理和人力资源专业人士在内的管理人员提供对权限和其他用户访问功能的控制的系统。

IBM 根据 IBM 安全解决方案 “Secure by Design” 计划的原则提供业界领先的解决方案，以满足可扩展的身份管理需求。Secure by Design 计划旨在帮助在 IT 基础架构内从头开始构建安全性，有助于组织将安全性融入它们提供的服务的结构中，使安全性成为业务流程和日常运营的一部分。IBM Tivoli® 身份管理安全产品通过针对用户管理、资源保护以及审计和合规报告的解决方案支持 Secure by Design 计划。

IBM Tivoli Federated Identity Manager 提供组织可以提供给其外部组成的企业-消费者自助注册和联邦单点登录(SSO) 支持等功能。IBM Tivoli Identity Manager 是一个自动化、基于策略的解决方案，管理组织内整个 IT 环境中的用户访问生命周期。IBM Tivoli Security Policy Manager 允许组织集中细粒度安全策略管理，跨应用、数据库、门户和商业服务执行访问控制。

整个用户生命周期内的安全性和合规性

有效的身份管理解决方案能够满足广泛的在线业务需求，从通过提供对更多信息和服务的访问来保持竞争力的压力到通过控制和监控信息访问来展示合规性的要求。该解决方案应该包括用于限制用户只访问与自己的角色和/或工作职能相适应的资源、集中用户自助服务、简化管理和审批处理、对用户访问权限进行周期性验证的工具以及策略控制文档。此外，还有管理账户配置和取消配置的成本上升、访问权限的重新认证、咨询台呼叫、密码重置及其他管理任务的需求。

随着组织为不同类型的用户授予访问权限，包括员工、客户、业务合作伙伴和供应商，它们需要能够支持整个用户身份生命周期的最佳实践解决方案，从新用户的高效加入到他们最终离开，以及消除不明或“孤儿”账户。

在外部，它们需要安全的、易于使用的解决方案，将对组织 IT 员工的管理需求降至最低。

在内部，它们需要创建用户账户，使新员工或担任新职能的员工能够尽可能发挥生产力。为了避免潜在的安全风险，它们需要快速收回离职员工的账户及相关的访问权限。

云计算环境通常支持大规模且多样化的用户社区，因此安全控制特别重要。必须提供身份联盟和快速加入功能，以协调身份认证和授权与企业的后端或第三方系统。需要基于标准的单点登录功能，以简化最终用户登录到内部托管的应用和云计算，从而使最终用户能够轻松、快速地利用云服务。

当涉及合规性时，组织需要企业范围的功能以确保内部和外部访问都通过有效的身份认证功能进行控制，从而监视授权和网络流量，通过综合的审计和报告功能为系统提供支持。

无论用户类型是什么，该解决方案都应通过帮助填补安全措施的空白加强安全性。它应降低欺诈、窃取知识产权或客户数据丢失等问题的风险。它应通过简化业务和 IT 流程，授予用户对资源的访问权限，帮助降低成本。

身份和访问管理环境下的成功之路

每个组织都必须确定确保有效的身份管理的详细信息，因为每个组织都有自己的需求、目标和用户群。然而，身份和访问管理的领先用例通常分为三类：

- 大量用户人群基于门户访问信息
- 用户访问基于云计算的服务
- 业务合作伙伴访问和应用集成

对于每种情况，组织都正转变它们提供访问的方式。为了实现这种转变，它们通常提供自助服务功能，因为这有助于确保安全操作并支持法律合规。

对于基于门户的情况，随着银行、零售和公共部门组织增加其在线运营的增值服务，基于门户的场景在数量在复杂性方面快速增加，组织不仅要应对安全性、可扩展性和可用性问题，还必须管理应用集成的后端任务。部署面向服务的架构 (SOA) 解决方案的组织需要一种有效的基于策略的方法，将安全管理和可以与现有 SOA 组件进行集成的服务融合在一起。

用例 1：针对大量用户人群的基于门户的访问

大型国家医疗信息交流门户需要为 300 万消费者和数百名付款人和相关的提供商提供对临床和管理数据的访问。它还必须支持医疗机构、设施运营商和保险公司之间的安全合作。它需要能够集中管理用户身份认证的解决方案，以确保在其安全扩展消费者、付款人和提供商的访问权限时能够保护患者记录的隐私。为了确保身份管理和执行访问控制，该解决方案必须支持遵从健康保险流通与责任法案 (HIPAA) 安全法规和更新的医疗信息交换 (HIE) 要求。

Tivoli Identity Manager 如何提供帮助

通过角色、账户和访问权限的使用，Tivoli Identity Manager 有助于自动化整个用户生命周期内创建、修改和终止用户权限。对于需要访问公司内部资源的企业内部用户和业务合作伙伴或可信赖的供应商， Tivoli Identity Manager 使组织能够授予访问信息和应用的权限，然后在用户角色和职责发生变化时控制访问。用户被授予密码重置等领域中的自助功能，但是根据角色 /岗位需求定义访问权限以及避免利益访问冲突的详细工作流和流程使 Tivoli Identity Manager 成为最适合用于有效的内部身份管理的解决方案。

Tivoli Federated Identity Manager 如何提供帮助

对于企业对企业和企业对消费者场景，在这些场景中，组织扩展了对大量外部用户的访问，Tivoli Federated Identity Manager 提供了自助注册功能，如选择密码以及密码问题和答案，以及联邦单点登录和集中的身份认证支持，以支持访问控制。这种自动化的用户验证减少了 IT 管理人员的工作量。

Tivoli Federated Identity Manager 可以扩展与业务合作伙伴的协作。这些业务合作伙伴需要通过提供入门级联邦功能和在需要时扩展到大量应用和用户来限制对内部资源的访问。结果是：降低了身份管理成本，提高了合规性和报告，简化了包含对软件即服务的集中的用户访问在内的服务集成。

用例 2：对基于云的服务的用户访问

一家全球性金融服务公司，拥有 120,000 名员工、300 万外部用户和在 50 个国家运营，实施了云计算架构，以标准化其 IT 基础架构和服务。在该流程中，该公司

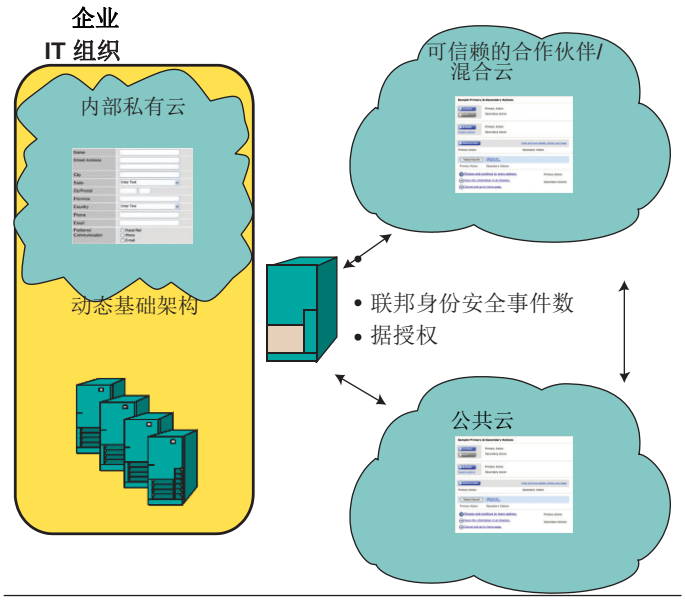
将数个数据中心整合到几个下一代数据中心。混合云解决方案借助不同的服务器、Web 2.0 服务目录内的自助要求驱动的配置和基于角色和业务需求保护对服务的访问，为企业在一个单一平台上提供自动化、虚拟化的基础架构。

为了在其新的基于云的数据中心实现安全管理，组织实施了 IBM Tivoli Federated Identity Manager，确保与业务合作伙伴的协作，并为外部用户提供对混合云环境的单点登录。

同样，一个跨 25 个团队拥有 2,000 名软件工程师的组织实施了开发人员云环境，为团队随时随地提供对服务的按需访问。用户登录要求功能，包括操作系统、内存、磁盘空间、中间件等，以及在数分钟内获得访问。

为了使用户能够安全、动态地访问并消除提供访问的滞后时间，组织实施了 Tivoli Identity Manager。过去密码重置需要数小时或数天才能完成，现在则只需几分钟，这是由于用户可以登录到自助服务门户，并自己重置密码。随着新成员加入团队，他们能够快速访问服务，在成员离开团队时，IT 人员只通过一个命令便能删除这些成员对所有系统的访问权限，而不必登录到几十个不同的系统。

保护对基于云计算的应用和服务的访问安全



借助 Tivoli Federated Identity Manager，组织能够集中控制大量用户对其基于云的服务的访问，这些基于云的服务通过 salesforce.com 等外部供应商托管。

Tivoli Identity Manager 如何提供帮助

允许内部用户访问基于云的应用在本质上与提供对其他应用的访问是一样的。Tivoli Identity Manager 提供的身份管理功能使组织能够为内部用户（包括特权用户）提供自助服务和对基于云的服务的访问权限。

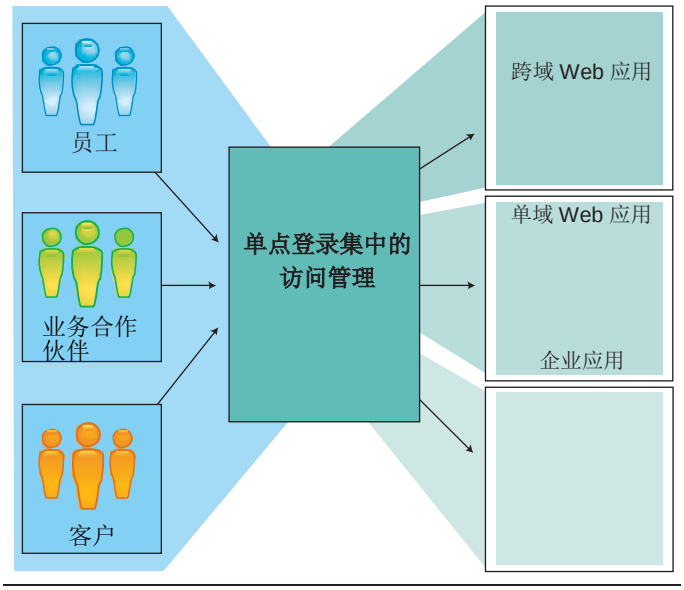
Tivoli Federated Identity Manager 如何提供帮助

使用基于云的计算通过互联网向大量用户（从组织其他部分的员工到客户和业务合作伙伴）提供应用和数据，需要特别注意安全性。 人数越多，管理用户身份就越困难。然而，通过 Tivoli Federated Identity Manager，组织能够集中管理和执行对内部和外部应用和服务（包括与软件即服务和基于云计算的解决方案的集成）的访问策略，并降低 IT 管理成本，同时帮助企业加强和自动化用户访问权限。

在典型的场景中，对用户的身份认证在云外进行，并涉及用于电子商务的 IBM Tivoli Access Manager（用于强认证）。然后利用 Tivoli Federated Identity Manager 将用户的身份联合到云中（用于面向用户的登录）。整个流程对用户是透明的。Tivoli Federated Identity Manager 的单点登录功能使用户能够直接进入基于云计算的应用和信息，而无需在云内管理身份。Tivoli Federated Identity Manager 包包括用于电子商务的 Tivoli Access Manager 以支持该场景。此外，IBM 还提供了Tivoli Federated Identity Manager Business Gateway，它提供了独立的功能，支持联邦单点登录和集成到云计算和软件即服务产品中。

用例 3：业务合作伙伴访问和应用集成

保险公司正在将其传统的、基于主机的应用迁移到新的基于门户的解决方案，需要向外包服务提供商、移动代理和客户提供关于其策略和合同的信息。组织还需要基于角色和其他属性对保险单和合同的细粒度的授权访问。 对合规性和数据安全问题的关注使组织部署 Tivoli Federated Identity Manager 和 Tivoli Security Policy Manager，实现内部和外部用户轻松、安全的单点登录功能，确保整个企业内的可审计的记录，并在须知的基础上执行数据级服务控制。



单点登录能够简化用户对多个应用和数据源的访问。

Tivoli Federated Identity Manager 如何提供帮助

Tivoli Federated Identity Manager 简化了应用集成，用于通过身份仲裁服务进行身份管理。该解决方案不需要数层访问便能访问应用，一次便能对用户执行验证、转换和身份认证，以提供应用访问，包括访问传统主框架 Java™和基于 Microsoft® .NET 的应用。对于需要特别访问安全信息的企业用户和业务合作伙伴，当身份被映射到访问用于审计和合规性时，通过身份管理能够提供一个记录。

Tivoli Security Policy Manager 如何提供帮助

Tivoli Security Policy Manager 为组织提供了在须知基础上管理和执行细粒度授权和数据级访问控制的功能。对于保险公司，Tivoli Security Policy Manager 允许移动员工根据角色和其他业务属性和背景访问客户合同，以确保隐私和数据安全。

针对内部和外部用户的 IBM 自助解决方案

IBM'的身份管理解决方案 Tivoli Identity Manager 和 Tivoli Federated Identity Manager，提供了自助功能，以简化对内部和外部访问信息和应用的管理。结果非常显著， 的新员工账户的配置时间减少达 80%，身份管理行政费用降低达 40%，咨询台收到的与密码相关的呼叫减少达 35%。[1]

Tivoli Identity Manager 提供了完整的身份生命周期管理功能，支持整个周期内的注册、权限和访问控制，在该周期内，一个人受雇于某公司，管理功能也适用于业务合作伙伴、供应商和需要信任地访问内部资源的其他外部人员。该解决方案结合了角色管理和用户配置，向用户提供访问权限。此外，分层角色结构简化了管理，提供了对用户对基础架构资源访问的可视化。用于管理角色、账户和密码的 Web 自助服务通过使用户自己执行任务，进一步简化了管理并降低了行政成本。自助服务请求可以配置为定义允许哪些属性可以自助，哪些属性需要获得许可。这是大容量、大规模 Web 环境的理想选择，在这种环境中用户的确切身份是未知的。

如果必须访问自己组织以外的资源，Tivoli Federated Identity Manager 提供高度可扩展的企业到消费者的自助解决方案，用于注册和身份认证，其中：

- 外部用户发起注册并选择密码
- 组织自定义挑战/响应、强大的身份认证和访问应用程序。
- 用户在不需要账户时便将其删除。

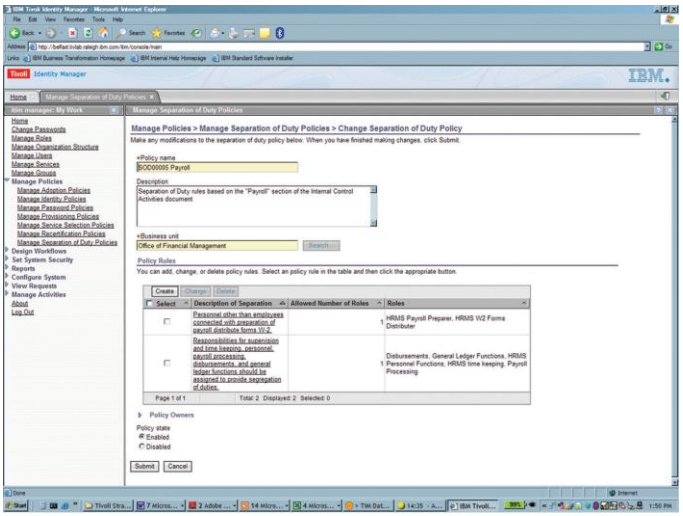
Tivoli Federated Identity Manager 提供了联邦单点登录和用户访问管理技术，跨组织边界进行集成时需要这些技术。

该解决方案提供了身份信任管理框架，使组织能够了解谁连接到资源，他们正在使用什么凭证，而无需单独管理用户。这是保护资产的理想选择，其中用户通过互联网或其他安全性较差的环境从接入点连接到关键资源。

这两个解决方案既可以单独部署也可以一起部署。当 Tivoli Federated Identity Manager 与 Tivoli Identity Manager 一起部署时，这种结合可以提供对扩展的应用和服务集合的访问。组织还可以采用分阶段实施，逐步增加支持的用户数量。 这使组织能够通过较少的
初始用户集证明该解决方案的商业价值，然后随着时间的推移扩展支持的用户数。

Tivoli Identity Manager

这种自动化、集中的、基于策略的解决方案利用角色、账户和访问权限在整个用户生命周期内管理用户访问。使用用户自助服务、委托管理、自动化许可处理、对访问权限的周期性验证及控制文档，它可以帮助提高用户工作效率，降低 IT 管理成本，实施安全性并管理合规性。Tivoli Identity Manager 旨在通过简化用户加入和离开并报告用户活动和持续的访问认证，从而降低成本，减少风险。



Tivoli Identity Manager 是在整个用户生命周期内进行身份管理的集中源。

Tivoli Identity Manager 帮助组织应对身份管理的主要挑战：满足内部和法规合规要求，保持有效的安全结构，实现可观的投资回报。

通过 Tivoli Identity Manager，组织能够：

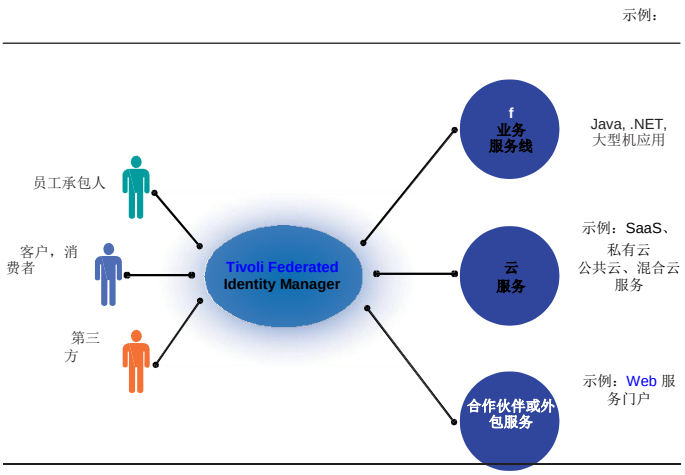
- 通过简化的群组管理和批量用户重新认证简化并降低管理成本。
- 减少安装时间，通过简化的策略、工作流和配置进行培训。
- 利用集中的密码管理支持增强的安全性，并降低帮助台成本。
- 自动或通过周期性访问重新认证工作流纠正和/或删除不合规的访问权限。
- 通过职责分离增强安全性和合规性。
- 通过预定义的模板定义工作流和配置的流程。

职责分离功能通过创建、修改或删除一些策略能够加强安全性和合规性，这些策略使用户无法获得多个角色的成员资格，因为这可能导致业务冲突。例如，拥有应收账款角色的用户不能同时拥有应付账款的角色。这种预防性方法首先可以防止入侵。

Tivoli Identity Manager 支持基于角色的配置，根据企业策略和个人职责授予访问权限，也支持基于请求的用户配置。它自动将用户的访问请求路由到适当的管理员，获得批准。由此产生的灵活性帮助组织管理快速、安全地执行用户访问。它支持在数分钟内对新用户进行配置，而无需数天内时间，使他们能够尽快发挥作用。

Tivoli Federated Identity Manager

Tivoli Federated Identity Manager 提供了集中的基于标准的 Web 访问管理系统，以管理和执行用户身份认证，单点登录和用于在企业内进行企业对企业、企业对员工以及企业对消费者部署的自助服务。 对于许多消费者与数百万企业连接和互动的场景，这种以用户为中心的解决方案降低了配置和管理用户账户的复杂性和费用。



Tivoli Federated Identity Manager 为组织外的用户提供了对服务的易于使用的自助访问。

Tivoli Federated Identity Manager 帮助组织建立了一个框架以了解哪些用户连接到了服务，使用了什么凭证来进行连接，而无需管理单个用户。

通过 Tivoli Federated Identity Manager，组织能够：

- 通过初始密码选择、密码变更/重置以及自定义客户特定需求的挑战/响应功能，支持针对企业对消费者的用户自助服务和移动用户场景。
- 通过多个基于开放标准的身份和安全令牌，管理用户身份认证和识别关于业务合作伙伴的信息。
- 通过管理、映射和传播用户身份降低行政成本，建立信任并促进合规性。
- 简化组织和其业务合作伙伴网站之间的集成，以降低安全风险。
- 通过单点登录功能管理和执行对多个服务的访问，以改善用户使用 Tivoli Access Manager 进行电子商务的体验。
- 通过 Tivoli Federated Identity Manager Business Gateway 提供针对云计算和“软件即服务”场景的联邦单点登录。

Tivoli Federated Identity Manager 提供了自动化功能，用于创建账户，创建或修改用户配置文件，创建和更改密码或密码问题。基于策略的集成安全管理支持 SOA 服务，安全管理被简化，用于跨公司的业务流程。

IBM 安全管理解决方案产品组合

Tivoli Identity Manager 和 Tivoli Federated Identity Manager 包括在 IBM Tivoli Identity and Access Assurance 里，这一更广泛的解决方案在支持合规性的闭环过程中也执行并监控访问。

Tivoli Identity and Access Assurance 提供针对用户账户的自动化的基于策略的管理，集中了应用授权，并提供了联邦单点登录功能。它为业务关键型应用、文件和操作平台提供安全的基于策略的访问控制。对用户活动进行自动监控、调查和报告。

IBM:领先 IT 安全解决方案值得信赖的合作伙伴

Tivoli Identity Manager 和 Tivoli Federated Identity Manager 是综合的 IBM 安全框架的组成部分，这一软件、硬件和服务的组合帮助组织应对用户和身份、数据和信息、应用和流程、网络、服务器和端点以及物理基础架构的安全挑战。IBM 安全解决方案促进智慧地球物联化、互联化和智能化的 IT 运营，提供整个 IT 基础架构的实时可视化、集中控制和增强型安全性，帮助客户解决成本、复杂性和合规性问题。

更多信息

如需了解关于 Tivoli Identity Manager、Tivoli Federated Identity Manager 和 Tivoli Security Policy Manager 或 IBM 安全解决方案的更多信息，请联系 IBM 销售代表或 IBM 业务合作伙伴，或访问：**ibm.com**/security

关于 IBM Tivoli 软件

IBM 的 Tivoli 软件可帮助组织有效地管理信息 IT 资源、任务和流程，以满足不断变化的业务要求，提供灵活且响应能力强的 IT 服务管理，同时降低成本。Tivoli 产品组合囊括安全性、遵从性、存储、性能、可用性、配置、运营和 IT 生命周期管理软件，并且以世界级的 IBM 服务、支持和研究团队为坚强后盾

。

IBM 客户负责确保其遵守相关法律要求。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或法规。

[1] 基于 IBM 从已安装系统获得的体验得出的结果和节省的成本。

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

在美国印刷
2011 年 1 月

TIW14069-CNZH-00