身份和访问管理解决方案买方指南：购买标准

Tivoli. software

IBM

选择正确的身份和访问管理解决方案

消除创新障碍

March 2008

全球各地的商业领袖都在更新他们对于尖端增长的关注——他们将创新视为达成此目标的手段。创新应如何出现？通过消除协作式工作环境的阻碍，使员工、客户和合作伙伴随时可访问关键资源，并有效地加以利用。

但在力所能及的范围内推动创新的访问同样也会给组织带来严峻的考验。每一天，组织都要面临着多重内部和外部的安全隐患。除了这些真正的隐患之外，还存在一个更大的挑战：需要保护业务系统的使用，并避免敏感业务数据的泄漏，以符合企业和政府要求。如果没有严格的控制，商业价值就会因客户缺乏信心、业务中断和企业或客户数据被窃导致的无法创新而迅速蒸发。为了保护业务完整性并促进遵从性，组织必须：

- **验证访问资源的所有用户的真实性。**
- **根据恰当的使用策略以及遵从法规的要求监控这些访问。**
- **在出现违规时，采取合理措施。**

急需一种安全性管理解决方案，帮助保护资产免受未经授权的访问，在不降低生产力的前提下完成此任务。这就是企业求助于身份和访问管理解决方案的原因。

身份和访问管理可以回答两个关键问题：您是谁？您可以访问什么？组织应该能够有效地跨多个领域回答这两个问题：数据、流程、应用程序、网络和其他端点以及物理基础设施。但组织往往有着耗时、低效的手动流程，用于定义、实现、维护和审计身份和访问策略，例如：

- **在各应用程序和数据库内构建安全性。**
- **在无数目录、数据库和文件中管理各种格式的用户信息。**
- **为数百个位置的众多相同用户管理安全性规则。**
- **需要多个密码。**
- **通过电子表格和其他文件手动检索和创建关键（但难以彼此关联的）遵从性和审计信息。**

这份买方指南帮助您选择正确的解决方案，帮助管理和控制企业内部和跨企业的访问。文中从CSO、IT操作人员、业务线经理和企业架构师的视角列举了组织所面临的最常见的身份和访问管理挑战。随后还概述了直接应对各挑战的组件，帮您评估特定厂商的解决方案是否能够最好地应对您的优先挑战。

身份和访问管理入门

在选择身份和访问管理解决方案时，应注意以下这些主要类别：

1. **在整个生命周期内管理用户和用户信息**
2. **确保高效访问有效的资源，最大化用户生产力**
3. **跨所有应用程序、数据源、操作系统和企业边界一致地管理和实施访问控制策略**
4. **通过身份治理监控和验证谁有权访问什么**
5. **加速价值实现进程**
6. **选择正确的安全性提供商**

对于每一个类别，您都会看到一份一览表，可在评估厂商及其产品时使用。

1．在整个生命周期内管理用户和用户信息

IT员工要付出大量时间管理用户特权和策略，这些内容可能存在于数百个不同的位置。以来一个处理一个的方式添加用户权限可能要耗费几个小时乃至几周的时间。删除用户权限也要耗费同样长的时间，还会带来遗漏本应停止访问的应用程序的风险。

为了消除无效的访问路径，IT团队必须始终手动审计所有生产服务器和应用程序。每当有人更改作业、角色或就职状态时，其所有现有的用户账户都必须得到合理的更改或删除——跨所有应用程序、操作系统和其他系统。

杰出解决方案的特征：	IBM	其他厂商
提供单一、安全的身份存储库	√	
提供基于Web的集成化界面，包含简单的向导和丰富的配置编辑器，使您能够轻松创建、修改和查看配置对象及其关系	√	
交付灵活的账户采用方法，这是安全有效地将账户映射到用户所必需的	√	
支持基于角色、基于规则和基于请求的供应用例	√	
提供核心角色管理和责任划分能力，提供与连续业务控制系统集成的开放接口	√	
支持工具使用基于简单向导的导航和用于较高级业务流程的拖放式GUI来构建用户供应工作流——均通过一个通用的Web界面完成	√	
跨异构数据存储库同步身份数据，这些存储库根据需求接收不同的授权信息	√	
将从权威源接收到的身份数据修改复制到其他需要利用这些数据的数据库和目录中	√	
管理分布式用户集合，包括为这些用户分配一种或几种角色的能力	√	
以随需应变的方法自动协调账户，从而迅速、可靠地发现“孤儿”（无效）账户，并启动自动或手动的补救流程	√	
自动化用户的登记，从入职到离职	√	
利用身份集成功能来建立规则，确定哪些组和个人有权更改哪些数据字段	√	
维护准确的配置和用户访问权限更改记录，以便用于审计	√	
提供对操作工作流的访问，允许定制供应活动	√	
支持供应内部网和外部网位置文件	√	
支持开箱即用的手动服务，使您可以快速轻松地自动化业务流程，治理目标，同时依然手动执行实际的供应任务	√	
支持开箱即用的手动服务，使您可以快速轻松地自动化以电话订购和其他手动管理项为中心的业务流程	√	
提供可定制、基于角色的用户GUI，具有经理、最终用户、审计人员、帮助台等角色的视图	√	

集中、自动化的解决方案使您能够更有效地掌控管理用户身份、凭据、账户、访问权限和审计的任务。自动化能够降低IT员工完成重复任务的成本，同时能够确保安全性得到了一致的管理。IT员工将从为所有应用程序构建安全性的繁琐任务中解放出来，指派解决方案来管理安全性——从而以最低的成本实现高度有效的安全性。

2．确保高效访问有效的资源，最大化用户生产力

为员工提供及时、直接的有效信息、应用程序和服务访问能够提高员工生产力。承诺新价值和增长机遇，向客户和合作伙伴敞开门户。合法用户数量的不断增加带来了严峻的安全性和实用性挑战。如果安全控件阻塞用户访问所需资源，或者要求经过多次登录和身份验证，用户就不会满意，不能获得较高的生产力。

输入、更改和重设密码占用了员工和IT管理员的更多时间。跨本地、基于Web和远程系统的单点登录（SSO）功能以及身份和访问控制解决方案可最小化密码相关问题的数量：

- **多个密码造成的混淆**
- **在人们写下密码时造成的安全性泄漏**
- **最终用户无法登录账户时所体验到的宕机时间**
- **IT员工耗费在密码管理方面的时间**

联邦SSO功能使用户能够使用SSO无缝地跨域边界的Web站点导航。联邦SSO功能减少了挫折和用户管理成本，促进了与合作伙伴组织之间的无缝协作环境。

自助服务功能可进一步改进用户体验，允许用户管理自己的账户、重置密码。利用这些功能，用户即可迅速准备好重新运行，而无需为呼叫IT帮助台而付出额外的时间和成本。

解决方案应提高生产力。 确保您选择的解决方案有以下特征：	IBM	其他厂商
提供直观、可定制的管理GUI，即指即点的功能允许您轻松创建新的用户GUI视图	√	
管理GUI内包含多重作业特性，允许您启动一个作业、打开第二个作业，然后切换回初始作业并完成它	√	
提供一种应用架构，使用一种GUI，可在其中执行所有管理职能	√	
允许您在一个GUI内提交和跟踪状态请求，监控工作流作业	√	
交付了向导和模板，可迅速轻松地进行配置，轻松访问为细粒度定制而生成的脚本	√	
使用用于多种身份验证解决方案的归档集成路径提供开箱即用的身份验证集成	√	
提供完整、集成化的联邦和信任管理解决方案，包含通用的安全令牌服务，用于Web服务/SOA环境内基于标准的身份传播	√	
提供与IBM WebSphere® Enterprise Service Bus的强大集成，促进和保护ESB的安全联邦访问	√	
包含健壮的目录、目录集成和同步成本——无任何附加费用	√	
通过工作流扩展自动化登录、密码更改和注销流程，推进自动化超越简单的SSO	√	
提供同一共向工作站上的快速用户切换，使一名用户注销、另一名用户登录，而宕机时间最短	√	
提供广泛的身份验证因素选择，包括用户ID和密码、USB智能卡、一次性密码、主动RFID和生物测定	√	
支持指派访问受保护资源所需的授权级别、在用户必须提供下一级别的身份验证时实施逐步完成的策略	√	
提供完全可配置的身份验证机制，附带外部身份验证界面，支持以任何语言编写的Web应用程序	√	
提供对本地和远程的全面端点覆盖；使用会话管理扩展SSO，包括对个人、共享（信息亭）、私有（信息亭与多重会话）、终端客户端、拨号会话、普适设备和漫游桌面的支持	√	
与身份服务器、应用程序、中间件、操作系统和平台广泛集成	√	

解决方案应提供对有效资源的高效访问。确保您选择的解决方案有以下特征：	IBM	其他厂商
跨Web应用程序等内容为用户交付SSO，包括IBM WebSphere、Microsoft®、Oracle和众多其他门户与应用程序环境	√	
为.NET环境应用程序提供直接的SSO支持，例如Microsoft SharePoint® 和 Exchange servers	√	
为Active Directory®（AD）实现密码更改、支持使用AD替代性userPrincipalName (UPN)电子邮件地址来验证，并将Active Directory Application Mode (ADAM) 作为用户注册库，从而简化Microsoft用户登录	√	
为跨站点身份验证支持多种标准，包括Security Assurance Markup Language (SAML)、Liberty Alliance and Web Services Federation Language (WS-Federation) 令牌传递协议	√	
支持Simple and Protected GSSAPI Negotiation Mechanism (SPNEGO) 协议，允许用户通过一次登录访问多个Web资源	√	
在解决方案中实现容错，而无需依赖可选的第三方工具	√	
为密码重置、密码同步和用户账户更新提供自助服务界面	√	
复制策略（而不是仅缓存）来提供高可用性，使策略在策略服务器宕机时依然能够正常实施	√	
利用Web授权方法，提供高性能，扩展到数千万应用程序的用户实现中	√	
提供灵活的Java™ EE基于Web的架构，可使用加固的反转代理或现有Web服务器的插件模块来保护资源（在某些情况下，专用代理可提供更高的安全性级别）	√	
提供久经考验的反转代理技术，经过超过1,000次客户安装的验证，从变更和配置管理的角度来看，非常出色	√	
包括会话管理服务，可限制各领域创建的会话数量、消除服务器重启、允许多个服务器实例共享用户会话，从而提高性能	√	
提供邮政功能，聚合如电子邮件、待办事项等，可根据您的选择进行配置	√	
支持轻量级联邦解决方案，允许较小的组织迅速与大型企业建立联邦	√	
支持企业到消费者（B2C）的联邦，使用新兴的用户中心身份，包括OpenID和Information Card Profile，使用Microsoft CardSpace或Higgins身份框架等身份选择机制	√	

解决方案应提供企业单点登录（ESSO）。确保您选择的解决方案有以下特征：	IBM	其他厂商
包括一个ESSO解决方案，其与多种不同应用程序协作的高级功能、与强大的身份验证的集成、会话管理的灵活方法、记录和审计最终用户活动的能力都使它在市场中卓尔出群	√	
包含领先的ESSO解决方案，它应该全面集成，由提供整个身份和访问管理套件的同一家厂商开发并支持	√	
提供一个ESSO解决方案，构建于Java EE架构之上，可轻松与身份、Web访问、联邦、强大的身份验证和其他安全性组件集成	√	
提供一个ESSO解决方案，包含多种会话管理功能，包括共享桌面、私有桌面和漫游桌面，促进迅速的用户切换集成广泛的第三方强力身份验证因素	√	
提供一个ESSO解决方案，与Web、桌面、电传和大型机应用程序以及Microsoft Windows® CE和Windows Xpe等客户端设备平台相集成，包容最广泛的应用程序	√	
提供一个ESSO解决方案，支持桌面密码重置功能	√	
支持ESSO，无需给目录基础设施带来额外的负载或影响目录模式	√	

3．跨所有应用程序、数据源、操作系统和企业边界一致地管理和实施访问控制策略

为了满足法规要求，组织需要保护数据和应用程序，确保访问此策略和数据泄漏规则跨所有应用程序、数据源和操作系统一致地实现和实施。有了这些功能之后，您就应该能够开展审计，证明和报告IT安全控制的有效性，同时准备好回答以下问题：

- **谁能够进入我的应用程序或数据库？**
- **哪里有哪些数据？因此我们应建立哪些访问控制？**
- **谁需要访问这些数据？**
- **我能否轻松证明用户仅访问了自己应该访问的内容？**
- **我能否有效地审计服务器上被访问的关键数据？**

正确的身份和访问控制解决方案会应用相同的业务策略来在整个组织内控制访问，包括针对跟踪系统管理员的高级审计跟踪。它提供了谁访问了哪些内容、为什么获得了相应的访问权限、这样的访问权限使用户能够做什么的闭环视图。这种可见性必须扩展到特权和受信任的用户，因为超级用户账户常会被滥用——往往对这些账户的访问权限没有任何控制，也无法审计使用这些账户的人们采取的操作。

理想情况下，您选择的身份和访问管理解决方案应处理使用正确的基于角色的访问权限注册新用户的完整生命周期，实施这些访问控制策略并检测和纠正任何尝试修改安全策略或用户权限的企图。

应选择具有以下特征的解决方案：	IBM	其他厂商
提供灵活、迅速配置、可扩展的身份提供方法，推送来自单一权威源的身份数据或从多个源拉取并聚合数据		
为业务经理和审计人员提供业务友好的描述，说明用户利用其访问权限能够做什么，从而帮助在新的访问批准请求、重新认证和审计评审中制订更好的决策		
允许管理员为细粒度资源应用有意义的描述，为快速引用和搜索进行分类，为它分配一个所有者，定义独特的批准和重新认证工作流，提供关于这些资源的详细报告		
具备无缝地与SAP和Oracle ERP集成的工作流，细粒度的责任划分检查与灵活的异常处理方法		
提供集中管理GUI进行控制和修改，消除手动更新各适配器以反映身份验证和授权方法更改的需要		
包含“what-if”策略更改模拟分析，可在做出更改之前确认哪些用户和权利将受到影响		
将业务规则整合到访问控制决策之中，在运行时评估这些规则		
在应用程序代码之外管理访问控制业务规则，允许您更改影响访问的策略参数，而无需重新和重新编译应用程序		
扫描应用程序漏洞，如跨站点脚本，在检测到漏洞之后帮助修复		
跨多个并发会话跟踪用户的行动，用户在一处注销之后，解决方案即可使其全面注销，以避免并发登录		
实施访问策略，用于不活动超时、三振出局规则和其他跨多个实施点的选项		
提供统一的策略管理，集中管理和控制访问，从操作系统资源到基于Web的应用程序SSO		
定义基于策略的规则，允许您轻松设置可用于不同系统、用户、存储或信息的安全策略		
设置访问策略，自动实时检测和纠正故意和无意造成的违规事件		
具有一个工作流，能够在提示的操作未完成时自动将工作流处理累加和重定向到另一参与者		
扩展到数千万用户，进行身份验证和授权，还可伸缩以满足内部网、外部网、Internet用户群的需求		
通过支持非标准、安全的IP负载均衡程序、通过复制服务器进行的智能化负载均衡和所含的集群支持提供可伸缩性和可用性		
利用SSL加速卡技术，保护硬件密钥存储，提供故障转移功能，允许自动切换到备份Web服务器		

4. 通过身份治理监控和验证谁有权访问什么内容

最有效的身份和访问管理解决方案采用集中、可伸缩的方法，跨所有应用程序交付久经考验的特性和健壮的安全性，以符合SOA设计目标。集中管理能够提供跟踪所有访问过系统的用户、协调根据业务优先事项和需求授予的访问程度的可见性，从而改进安全性工作的一致性。

为了跨复合业务应用程序和业务单元管理用户身份，企业架构师应能够创建通用的身份代理服务或“作为服务的受信任的身份管理”。这样做能够提高业务灵活性，可在业务需求变化时添加新服务或连接现有服务，而无需重新编写身份处理的代码。它允许业务线专家关注交付应用程序内需要的业务逻辑——而不必担忧应用程序本身的安全性。

企业架构师还应能够通过高效有效地跨SOA管理和供应用户身份的能力扩展企业服务总线（ESB）的功能。这种方法创建了一种“身份感知”的ESB，使企业架构师能够确保用户能根据其安全性凭据和访问级别获得对应用程序、数据和信息的访问权限——无论他们所访问的应用程序是什么。

应选择具有以下特征的解决方案：	IBM	其他厂商
提供真正的闭环策略遵从性实施，检测和补救在供应流程之外授予的访问权限，而不必完成可能存在多个故障点的复杂、多步骤的系列流程		
包括开箱即用的自动化、可配置、高级的证明/重新证明处理，帮助满足需求，例如Sarbanes-Oxley (SOX) 404访问重新证明要求		
利用单一、安全的身份存储库，从中可跟踪和审计所有身份事件		
提供单一身份GUI，通过它可执行所有管理功能，跟踪和审计身份事件		
自动提供所有活动的审计日志——包括管理活动（如策略修改），以开箱即用的方式提供		
包括工作流，作为解决方案的完整组成部分，使整个生命周期和供应事件都能被解决方案管理和监控，解决方案还可记录下所有事务数据，以便在依法审计和报告时使用		
建立中心框架，治理和保护您的SOA环境		
为各服务应用程序实施和治理恰当的访问控制		
跨不同的服务转换和映射一组不同的用户身份		
跨组织筒仓和防火墙管理特定于应用程序的身份		
建立身份信任管理框架，确保事务得到安全执行		
端到端地传播所需凭据——从联系点（如XML网关）通过ESB传递到后台（如ERP或大型机应用程序）		
跟踪和比较所有登录事件，允许您审计应用程序访问		
提供广泛的审计和细节报告，可将其提交给管理机构、外部和企业审计人员		
跨广泛的安全设备周边集中收集、简化和关联与安全性有关的事件和警告		
提供审计跟踪记录，说明谁有权访问什么、谁批准了相应的访问权限		
提供特权用户监控和报告		
为跨所有解决方案组件调度、分发、查看和定制报告提供一个通用的报告系统		

5．加速价值实现进程

在评估不同的身份和访问管理解决方案时，有必要选择一种提供快速的价值实现进程的产品。成本效益高的解决方案包含多种旨在提供轻松配置、集成和维护的关键特性。

应选择具有以下特征的解决方案：	IBM	其他厂商
所有必要的基础设施适配器，领先的中间件和软件组件商业版本，包括必要的数据库、LDAP服务器和Web与应用服务器		
功能全面、开箱即用的功能，无限制的组件版本，如工作流必须升级，这样才能使用所需的全部丰富特性		
同类最佳的目录和数据集成与同步工具，与解决方案绑定，可很好地应对任何集成挑战		
成熟、久经考验的功能，经过数百次全球客户安装的考验		
经验丰富的服务团队，可在实现过程中确保高生产力		
专门设计用于加速实现的工具		
提供教育和培训课程，使您的员工能够更快地获得高生产力		
解决所有异构目标需求的能力		
嵌入式集成业界领先的IBM WebSphere Application Server		
定制身份验证，可将现有基于Web的身份验证应用迅速集成到针对所有用户的身份验证流程之后，而无需借助第三方开发		
支持在一台服务器上完成安装，支持轻松配置，包括所有底层中间件		
与最新应用程序的广泛集成（包括PeopleSoft和Siebel），支持使用多个目录/用户存储库和异构中间件（包括Oracle Application Server）		
明确而直观的定价和许可费用，并非根据使用类型和其他额外收费的自选服务器、应用程序等定价		
支持本地语言，整合动态语言支持，显示特定内容的部署，如以各用户的首选语言显示的密码加密/响应问题或电子邮件通知		
策略、配置和框架的导入/导出功能，可加速QA和生产之间的系统推广，也适用于策略定义的版本控制		
平台支持的广度，包括Windows、UNIX、Linux on distributed、Linux® on IBM System z and IBM z/OS®		
定制自助服务UI的品牌形象（外观和感觉）以及布局的能力，在修订和升级之后保持定制效果，从而保护投资		
Evaluation Assurance Level 3或更高版本的通用标准		
标准配置和编程语言，而不是专用脚本或工作流定义语言		
用于监控身份和访问管理解决方案健康状况和可用性的工具		
自助服务密码重置，与服务台（帮助台）系统相集成，包括事故单的生成和结束		

6．选择正确的安全性提供商

您选择的提供商应该能够为您的身份和访问管理解决方案提供全面支持。理想情况下，您还希望提供商能够在您实现解决方案的整个过程中为您提供支持。在选择提供商之前，请务必提出以下问题：

厂商的安全性愿景是否与您的愿景一致？

理想的厂商应该与您一样重视安全性，也理解不够可靠的安全性基础设施会给您的组织造成怎样的影响。

厂商是否关注真正的企业安全性需求？

对于关注点过于狭窄，仅关注针对特定环境的一种解决方案的厂商，您可能会遭遇“安全性孤岛”问题。应该选择能够应对全局的厂商。

厂商是否通过其技术为您的业务目标提供支持？

理想厂商的解决方案应与您的业务目标一致。他们的解决方案是否提高了效率、缩短了业务服务部署时间、降低了成本、加速了推向市场的进程？

厂商提供整体解决方案的一部分还是完整的解决方案？

如果需要涉及多家厂商，解决方案的成本和管理多家厂商所需的时间会大大增加。理想的厂商应该拥有身份和访问管理的完整产品组合，包括UNIX®和大型机访问控制、Web服务安全性和联邦。

厂商的产品是否为提供无缝的功能而紧密集成？

解决方案集成得越好，手动集成技术所需的工作就越少。

厂商的客户支持情况如何？

厂商应该提供快速响应、高度有效的迅速客户支持。务必理解其逐级上报的过程，务必确保他们有能力将您的业务放在第一位，以这样的方式为您提供支持。

厂商的全球形象属于哪种类型？

如果您的组织有国际分支机构，就应该寻找有全球影响力、久经考验的国际业务经验的厂商。应确保厂商能够通过其当地资源为您的国外分支机构提供支持。

在您需要时，是否有可信赖、拥有足够的专业经验和带宽的成熟支持组织为解决方案提供支持？

理想的厂商应该有着久经考验的支持组织，可帮助您最大化软件投资的价值。

厂商的解决方案是否一贯受到分析家的好评？

理想的解决方案应该经过领先分析家开展的多维度独立分析和考察，且得到认可。

您对厂商的稳定性及其在当今激烈的经济环境中保持力量的能力是否有信心？

在当今的经济环境中，一个重大的问题就是厂商的稳定性和生存能力。理想的厂商应该有着在该行业中的长期发展史，有着可靠、长远的战略和安全度过经济艰难时期的资源。

厂商能否交付有着战略设计、技术超群的产品？

比较各种安全性解决方案时，应关注技术优越性——设计良好的功能性、智能化的架构设计以及对行业标准的广泛支持，例如Security Assertion Markup Language (SAML)、Liberty Alliance、WS-Federation、Service Provisioning Markup Language (SPML) 和 eXtensible Access Control Markup Language (XACML)。

携手IBM，满足您的身份和访问管理需求

开始评估身份和访问管理厂商时，您会发现，IBM不仅提供了同类最佳的解决方案，其安全性解决方案的广度和集成也是无与伦比的。只有IBM使您能够通过灵活、自适应的方法跨整个IT安全风险领域降低保护企业的复杂度，从而集中精力促进业务创新。在您准备好扩展到其他安全性管理领域时，IBM可随时支持您的长期安全性目标。

对于身份和访问管理周期的每一个阶段，IBM都提供了能达到杰出解决方案的所有标准的软件：

- **IBM Tivoli® Identity Manager软件使您能够快速供应用户身份，并在整个生命周期内管理身份及其访问权限，支持用户自助服务（例如密码重置）——完全向您的安全性策略看齐。**
- **IBM Tivoli Access Manager for e-business提供了企业范围内的端到端应用程序安全性，包括SSO、URL和应用程序级授权、基于分布式Web的管理和策略驱动的安全性。**
- **IBM Tivoli Access Manager for Operating Systems保护非结构化数据文件以及应用程序和操作系统资源，它能够建立规则来调优对所有UNIX和Linux账户的访问，包括特权用户账户，如超级用户和根账户。**
- **IBM Tivoli Federated Identity Manager在SOA和Web服务环境中交付了跨域或联邦SSO以及身份传播，支持可靠、便利、可审计的合作伙伴交互，解决了与其他域的合作伙伴访问相关的关键遵从性问题。**
- **IBM Tivoli Access Manager for Enterprise Single Sign-On帮助简化、扩展和保护最终用户对于Web和非Web应用程序的ESSO，使您能够优化生产力、降低与密码相关的帮助台成本并简化最终用户的密码管理工作。**
- **IBM Tivoli zSecure Suite联合IBM z/OS Resource Access Control Facility(RACF®)的管理、审计、警告和监控功能。设计用于帮助最小化安全性泄漏，流线化遵从性工作。**

这种广泛的身份和访问管理产品组合能提供支持当今需求所必需的基础设施。除了管理用户身份和资源访问之外，建立来自IBM的集中、自动化的身份和访问控制基础设施终将成为业务驱动因素，帮助您：

- **最小化响应多种内部和外部控制和法规的复杂度。**
- **通过捕捉、创建和自动化可重复工作的最佳实践来优化生产力和成本。**
- **使IT员工能够转而关注价值更高的活动。**
- **消除创新障碍，提供借助新业务机遇取得领先地位所必需的敏捷性。**
- **促进业务流程的完整性和机密性。**

更多信息

进一步了解适合您的企业的身份和访问管理解决方案，讨论IBM服务管理软件为您的组织带来的收益，请联系您的IBM销售代表或IBM业务合作伙伴，也可访问

ibm.com/tivoli/solutions/security

关于IBM Tivoli服务管理软件

Tivoli软件为组织提供了一个服务管理平台，通过提供可见性、控制和自动化来交付优质服务——查看和理解其业务运作的可见性；有效管理其业务、最小化风险、保护品牌的控制；优化业务、降低运营成本、更快速地交付新服务的自动化。与IT中心的服务管理不同，Tivoli软件交付了管理、集成和协调业务与技术需求的通用平台。Tivoli软件设计用于快速处理组织内最紧迫的服务管理需求，帮助前瞻性地响应不断变化的业务需求。Tivoli产品组合由世界级的IBM Services、IBM Support和IBM业务合作伙伴的活跃生态系统提供支持。Tivoli客户和业务合作伙伴还可参与全球各地独立运作的IBM Tivoli User Groups（请访问www.tivoli-ug.org），利用彼此的最佳实践。

IBM Corporation
Software Group
Route 100

Somers, NY 10589
U.S.A.

在美国印刷

2008年3月

TAKE BACK CONTROL WITH Tivoli.

TI014000-USEN-00