IBM软件

Tivoli software

面向云和SOA环境的IBM Tivoli Access Management

实现对新服务交付平台的安全访问

要点

- 通过了解谁连接到了内部和外部服务，加强安全性
- 降低添加新服务的复杂性，提高业务灵活性
- 支持端到端审计用户访问，促进合规性

企业如今正在不断寻求新的方式来有效且经济高效地交付应用和服务。许多企业已在使用Web服务或面向服务架构(SOA)的实施实现内部和外部应用的访问，同时越来越多的企业正在探索将云计算用作交付平台。这些传统IT基础架构的替代方案有助于降低IT和应用开发成本，增加协作机会和促进业务增长。然而，与此同时，它们也可能创造新的漏洞，将对应用和服务的访问暴露在传统企业边界以外。企业因此需要比传统IT更高的安全性来管理和保护对这些应用和服务的访问。

IBM Tivoli® Access Management解决方案专为在非传统交付平台(比如云和SOA部署)中实现对应用和服务的安全访问而设计。它们专门提供对以下各项必不可少的功能：

- 通过减少出现不一致的安全策略的风险，保护对内部和外部应用和服务的访问。
- 在SOA部署中管理用户访问，其中Web服务的引入将转变IT环境。
- 安全访问混合云部署，组织利用云的优势，同时仍然保护可能存在风险的敏感信息。

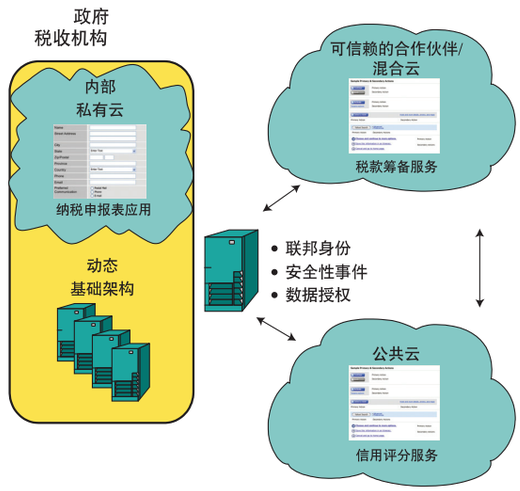
IBM

保障对内部和外部部署的访问的安全

许多公共部门组织，尤其是那些主要提供客户服务的组织，正越来越多地与其他组织交互、协作和交换数据，以便有效且经济高效地提供服务。例如，在下图所示的场景下，政府税收机构需要能够与可信赖的合作伙伴(如税款筹备服务提供商)和实体(如信用评分服务公司)合作和交换信息。在此场景中，无数的内部和外部用户将要求同时访问内部和外部应用。这些应用所处的环境包括软件即服务的部署和云计算。

在此场景中保障对内部和外部应用和服务的访问的关键是在现有的身份和访问管理基础架构上构建，并用其支持面向安全访问已转变的资源的可扩展和高度可用的解决方案。对现有基础架构的其他要求包括联邦访问控制和数据授权管理。这些使组织能够建立实现安全协作所必须的用户身份和组织级信任。例如，在下图中，在公共云中运行的信用评分服务提供商需要确保请求信息的一方确实如他们所自称的，是政府税收机构或税款筹备公司，而不是寻求未经授权访问个人信用记录中的信息的黑客。

保护对内部和外部应用和服务的访问



协作要求内部和外部用户安全地访问内部和外部应用。

联邦访问控制和数据授权管理也能减少对内部和外部应用和服务的不一致访问的风险。具体来讲，联邦访问控制简化了对不同安全域中不断增多的信息的整合过程，促进了对内部和外部部署中的应用的安全访问。数据授权管理提供了一种集中式方法来管理和实施安全策略，从而控制对数据和应用的访问。当部署多个应用和服务时，与实施不同的安全策略来分别控制对每个应用的访问相比，这种替代方法提供了巨大的优势。

保障SOA和Web服务部署中的访问的安全

许多组织正在实施SOA来转变它们的IT和应用环境，部署大量Web服务以支持业务需要。例如，在客户店内安装智能电表的公用事业企业正在向他们的技术环境中引入更多Web服务。安装智能电表的优势之一是运营效率更高，运营成本更低，因为智能电表可以直接把客户使用数据发送到公用事业公司基于SOA的IT环境，而不是要求它们的员工亲自出去读取电表。因为这些智能电表使用Web服务接口来传输此数据，所以这些Web服务必须在SOA环境内受到保护。

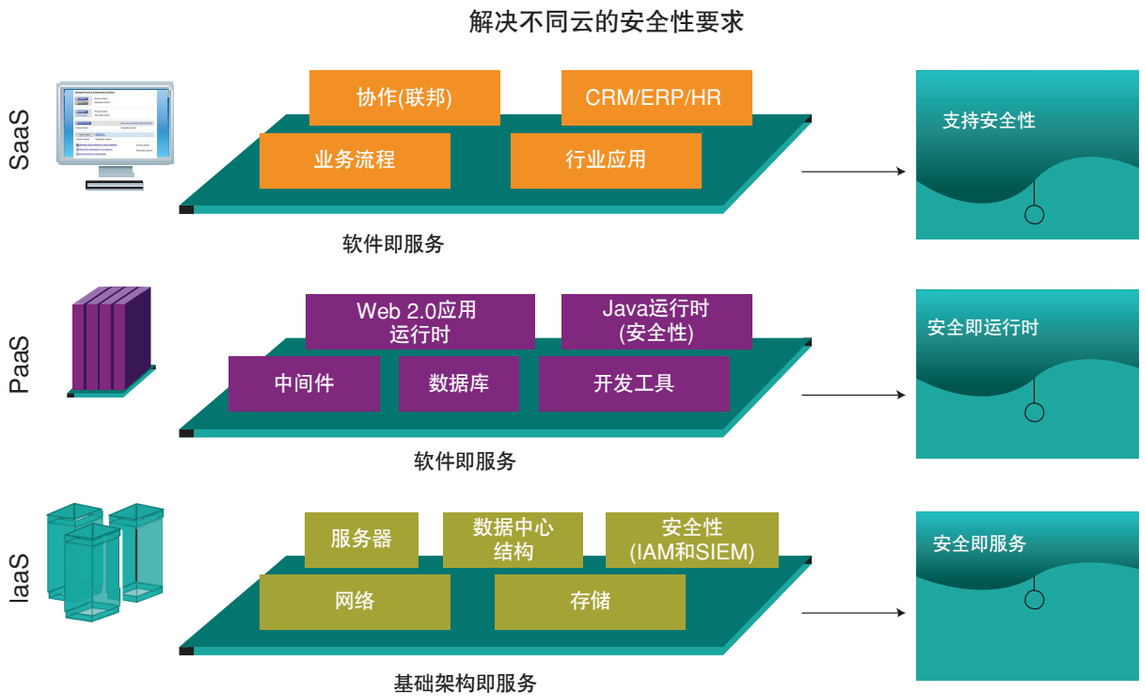
可以将安全性作为一项运营服务来提供，直接供架构内的应用和服务使用，从而保护Web服务。关键在于采用一种基于策略的方法将安全管理功能和运行时安全服务融合在一起，运行时安全服务可轻松地整合到XML防火墙、企业服务总线(ESB)和服务注册表及信息库等现有的SOA组件中。有效的安全策略管理必须包含消息保护和细粒度的授权管理功能，通过在应用和服务内集中管理和实施权限和数据级控制，加强数据安全。

在SOA环境中实现安全即服务，有助于公用事业公司和其它提供服务的组织推出新服务时，通过降低安全上线新服务的复杂性降低部署成本。

保障混合云和SaaS部署的安全

在整个消费和公共领域，云计算逐渐被证明是一种在互联网上提供IT服务的灵活且具成本效益的方式。云资源可以快速部署和轻松扩展，可以按需供应应用和服务，无论用户位于何处。这带来了诸多优势，比如能够提高服务交付效率，简化IT管理，以及将IT服务与业务要求保持一致。但对许多组织而言，这些优势也可以带来相关成本和风险：安全性的挑战。除了常见的开发安全的IT系统的挑战，云计算还由于重要服务常常在云模型中外部化而增加了风险。在混合云模型中，组织可以与云计算提供商合作托管他们的服务，同时保留数据的所有权。这要求对提供商和它们为组织的重要数据提供安全保护的方式拥有较高的信任水平。

有多种类型的云，但不是所有类型都具有相同的安全要求。云可以是私有的，在这种情况下云归一家组织所有；或者是公共的，在这种情况下云可供能访问互联网的任何人使用。在云模型中提供的服务类别包括软件即服务(SaaS)、平台即服务(PaaS)和基础架构即服务(IaaS)。许多组织选择结合私有云和公共云以形成一种混合云，以便满足具体的业务和技术要求。



不同类型的云可能具有不同的安全要求。

使用SaaS部署，安全管理的大部分职责都由云计算提供者承担，他可以充分利用多种方式来控制访问，包括用户身份管理。PaaS部署使部署云计算的组织能够承担管理中间件、数据库软件和应用运行时环境的安全性的更多职责。IaaS部署能够将更多的控制权转交给组织。在混合环境中，组织可以利用这些模型的优势，避免了公共云部署内在的安全风险。

要保障这些基于云计算的服务的安全，关键在于利用端到端的安全策略，汇集组织内存在的身份和访问管理基础(包括数据授权管理功能)以及在云计算中部署的联邦访问控制和运行时安全服务。要成功实现这一点，要求企业已具备数据中心网络和虚拟化安全性，以便将应用和服务迁移到云计算的过程具有内在的安全性。

安全性在云计算部署中扮演两种角色：使组织能够建立安全的基于云计算的服务部署，并在云计算中提供安全即服务，以支持正在为云计算部署而构建的新应用。面向混合云计算的实际安全解决方案是一种深度防御方法，能够应对将强大的内部安全功能用作扩展到云计算的基础的能力以及直接在云计算中使用安全即服务轻松运行访问联邦、授权管理和其它安全运行时实施功能的能力。

使用IBM Tivoli Access Management加强云和SOA的安全性

IBM安全解决方案提供了身份和访问管理基础架构中所必需的重要功能，保护对云和SOA环境的访问，包括以下产品。

*IBM Tivoli Federated Identity Manager*提供了联邦的单点登录(SSO)技术来保护用户对内部和外部应用和服务的访问，使用多种形式的用户凭证简化应用、SaaS和基于云计算的服务整合。它有助于可信赖合作伙伴之间的安全信息共享，并融合了身份调解服务来管理、映射和传送用户身份，而不必在云计算中加以管理。它支持众多以消费者和用户为中心的联邦功能，跨SOA和Web服务部署提供身份感知和可审计的访问。

*IBM Tivoli Security Policy Manager*是一个强大的数据和应用授权管理解决方案，为组织配备了集中的安全性策略管理和跨多个基于云计算的服务的分布式策略的实施。数据授权管理使管理和实施与不同的服务和应用相关联的数据安全策略成为可能，无需处理多个拥有特定产品定义的策略。通过快速部署Web服务，此功能有助于减少管理安全策略的时间和成本，并减少部署不一致的访问控制和对敏感数据的意外访问的风险。

IBM WebSphere® DataPower® SOA Appliances是连接和XML防火墙设备，有助于保障SOA和Web服务转变的安全并加速其转变。通过在SOA基础架构中提供按需整合的特性，WebSphere DataPower SOA Appliances成为了少数非停机的应用优化和整合技术之一。面向SOA环境的Tivoli Access Management解决方案旨在整合开箱即用和WebSphere DataPower SOA Appliances，并支持SSO的集中、用户会话管理和一致的安全策略管理，以帮助证明合规。

*IBM Security Virtual Server Protection for VMware*在保护云计算部署的服务交付的安全性的过程中，用作底层基础架构的一个重要组件。通过为虚拟化的数据中心整合和优化安全性，Virtual Server Protection for VMware帮助确保在应用和服务转移到云中时，虚拟化环境本身是安全的。

更多信息

要了解IBM面向云和SOA环境的安全解决方案的更多信息，请联系您的IBM销售代表或IBM业务合作伙伴，或访问：

ibm.com/tivoli/security

身份和访问管理服务

IBM的身份和访问管理服务(Identity and Access Management Services)可帮助您设计、实现、部署和维护一个整合的身份管理系统。这样一个系统可以在多个平台之间为用户、设备、应用和业务流程以及生物识别器、智能卡和标牌阅读器等物理身份验证点标准化访问管理。

此外，IBM Global Financing提供的财务解决方案能够实现有效的现金管理、保护资产免受过时技术威胁，提高总体拥有成本和投资回报。另外，我们的全球资产重新利用服务(Global Asset Recovery Services)能够使用全新的、高能效的解决方案帮助解决环境问题。关于IBM Global Financing的更多信息，请访问：

ibm.com/financing

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

在中国印刷
2011年11月

TIS14053-USEN-00