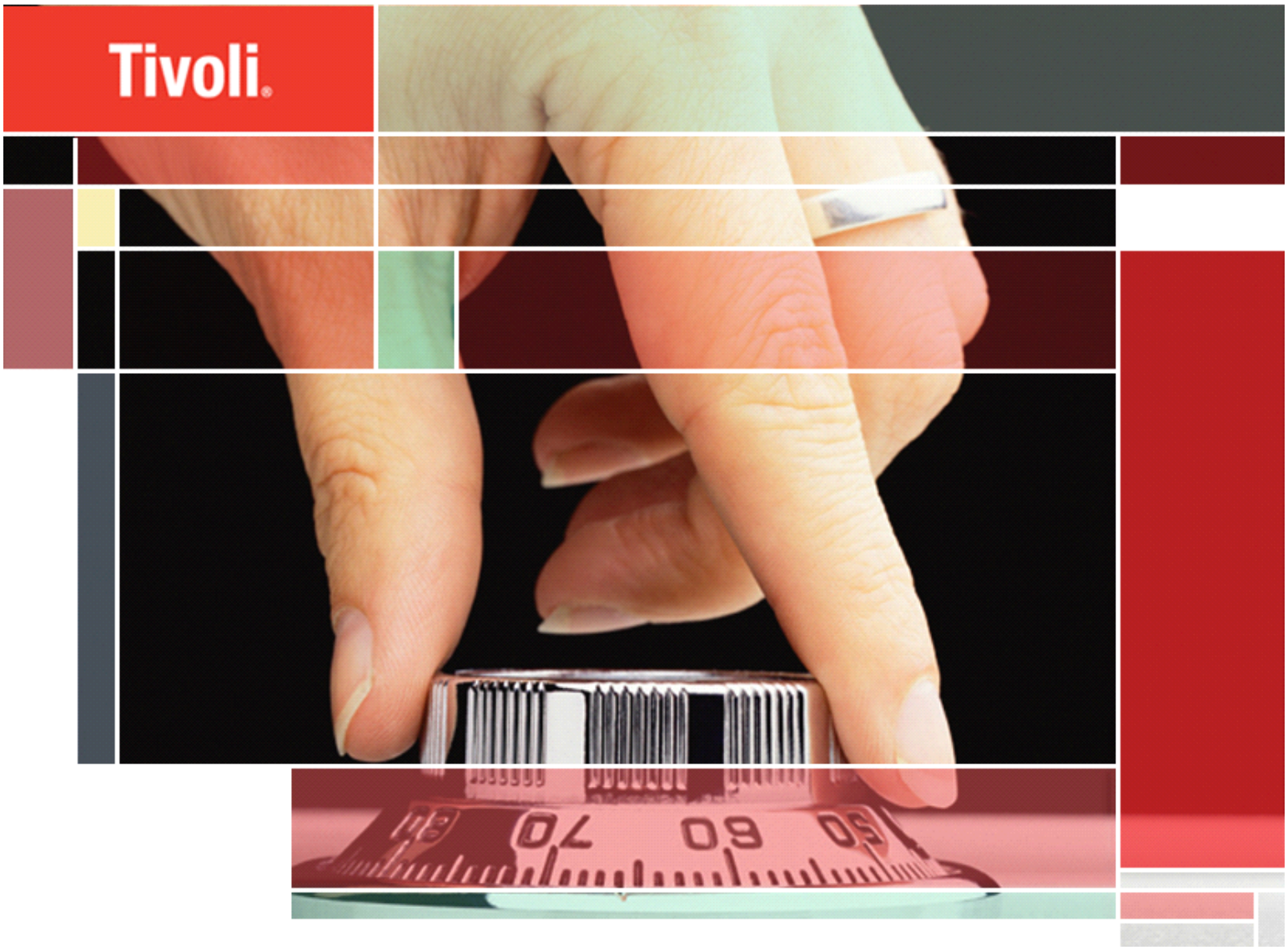
Tivoli. software




# IBM Tivoli 电信行业

# 身份管理与访问控制方案建议书

# 目 录

# 第 1 章 电信行业身份管理与访问控制需求分析

## 1.1 客户的需求与挑战

随着电信行业的迅速发展，应用系统不断增加，企业内部和外部的用户数量在指数级增长。企业在进行应用系统整合阶段，往往忽略了系统的账号信息整合。而系统整合的一个重要基础就是帐号信息的统一管理、集中授权、单点登录认证和身份安全审计。目前分散的账号信息管理、密码管理、授权管理模式，使得用户帐号管理、认证授权工作变得费时而安全漏洞聚集，主要表现在以下方面：

- 应用系统繁多，且不同的业务系统有独立的认证、授权和审计系统，并且由相应的系统管理员负责维护和管理。一方面造成用户帐号的创建，更改，删除流程复杂，在用户管理的工作量不断加大；另一方面用户需要记住不同的用户名和密码，不但用户使用不便，登录和认证信息的经常丢失也致使管理员工作负担加重。
- 由于缺乏统一的身份管理平台，难以管理系统运维帐号，超级用户帐号共享的现象普遍存在。账号的多人共用，不仅在发生安全事故时，难确定账号的实际使用者，在平时也难于对账号的扩散范围进行控制，容易造成安全漏洞。
- 每个系统分别管理所属的系统资源，为本系统的用户分配权限，缺乏企业全局的、集中统一的资源授权管理平台，无法严格按照最小权限原则分配权限，系统的安全性无法得到充分保证。
- 随着系统的增多，用户经常需要在各个系统之间切换，每次从一个系统切换到另一系统时，都需要输入相应的用户名和口令进行登录。给用户的工作带来不便，影响了工作效率。用户为便于记忆口令会采用较简单或相同的的口令，危害到系统的安全性。
- 由于各系统独立运行、维护和管理，所以各系统的审计也是相互独立的，缺乏集中统一的系统访问审计。无法对支撑系统进行综合分析，不能及时发现入侵和账号违规使用行为。

很明显，随着业务系统和系统的发展及内部用户的增加，IT 服务部门往往要消耗大量的精力进行用户帐号的维护管理，工作效率无法提高；同时，帐号的分散管理和信息不统一，无法对各业务系统实现统一的安全策略，从而在实质上降低了业务系统的安全性。因此需要集中统一的安全管理技术和平台。

## 1.2 IBM 安全身份管理和访问控制方案概述

针对电信业目前的用户管理和认证现状，我们建议建立集中的身份管理和访问控制平台，根据企业的身份管理策略和流程，实现所有系统管理员对于所有身份对象的集中的自动化管理和访问授权和控制，同时提供用户单点登录、用户信息自助管理和用户行为审计的功能。

### 1.2.1方案简述

IBM 身份管理和访问控制方案，一个得到国际，国内业界实际验证的身份管理平台，通过提供集中的用户认证和授权管理来构建应用的安全域，通过对所有系统中的账号信息进行整合，使得系统和安全管理人员可以对用户和各种资源进行集中管理、集中认证、集中权限分配、集中审计，从技术上保证安全策略的实施。用户还可用单一账号访问所有需要使用的系统。

IBM 身份管理系统统一了用户信息的管理工作和用户与实际业务之间的关系。身份管理的主要目的就是让用户更方便和更高效地建立用户在企业 IT 环境中的身份，使得用户可以尽早地使用企业的 IT 资源，为企业创造价值。它包括了用户身份的整个生命周期的自动化管理以及围绕用户管理的各种业务流程的自动化。

对于众多的最终用户而言，身份管理系统又提供了一个可以自我管理帐号信息的机制，一些简单的用户属性修改、用户口令修改等工作就可以让用户自己来完成，从而解放管理员在用户管理上的工作量。

IBM Tivoli 安全系列产品包括：

1）Tivoli Identity Manager实现统一身份管理；

2）Tivoli Access Manager作为统一认证，集中授权和单点登录；

3）Tivoli Directory Integrator用于数据集成的工具，提供元目录服务；

4）Tivoli Director Server作为集中身份存储的LDAP服务器。

### 1.2.2 方案价值

统一的身份管理与访问控制平台的价值体现在系统管理员方面、普通用户方面、系统安全性、系统管理费用等多个方面。从企业的不同角度出发进行安全身份管理并且价值显著：

- **企业角度**

在身份管理与访问控制平台框架下，账号、授权管理将纳入统一、账号设置、分配均有详细记录，可以审计；账号撤消、更改后的同步工作均由系统自动完成，无需手工同步。

### ➢ 管理员角度

采用集中平台，方便用户账号的整个生命周期管理。如账号创建、授权、权限更改、个人信息更改、口令更改、账号删除等，均可在一个平台上进行管理，使用户与其账号的对应关系符合实际情况，保证用户拥有的权限是完成其工作所需的权限。

集中平台还为安全策略的强制统一执行提供技术保证，如监测用户口令的强度，口令更改周期等等。减少由于用户忘记密码产生的维护成本。这些都使管理员对信息资源管理的效率大大提高。

### ➢ 用户角度

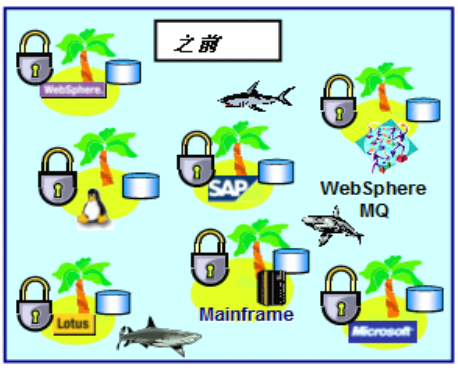
通过集中平台，可以保证用户权限的分配符合安全策略要求，拥有完成任务所需要的最小权限。用户可以通过该平台提供的自助管理接口，可以方便地更改自己的口令和个人基本信息，提高了用户的工作效率。

通过访问控制的单点登录功能，用户一次登录即可方便地访问被授权的所有系统，省去了记忆多个账号名和口令的麻烦，提高了工作效率。

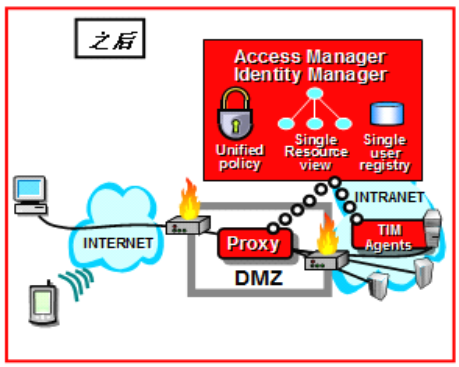
### ➢ 系统安全角度

通过集中平台，一个指令，即可以干净、彻底的清除与每个用户相关的所有账号，防止出现用户已经离职但账号还存在的情况。另外身份管理与访问控制平台为安全策略的强制执行提供了技术手段，如单点登录系统可以为用户在不同应用系统中自动设置足够强的口令，并且可以自动定期修改口令。这种设置和修改对用户是透明的，用户只需记住登录到单点登录系统的口令即可，提高了用户的效率，防止弱口令的存在。

IBM Tivoli 系列安全产品可以帮助企业构建整个企业的安全平台，并实现核心企业收益：




- 太多的口令需要记忆
- 多个管理员，多个管理工具
- 工具不能一起工作
- 到处都是用户信息和控制信息
- 安全成为应用开发者的任务

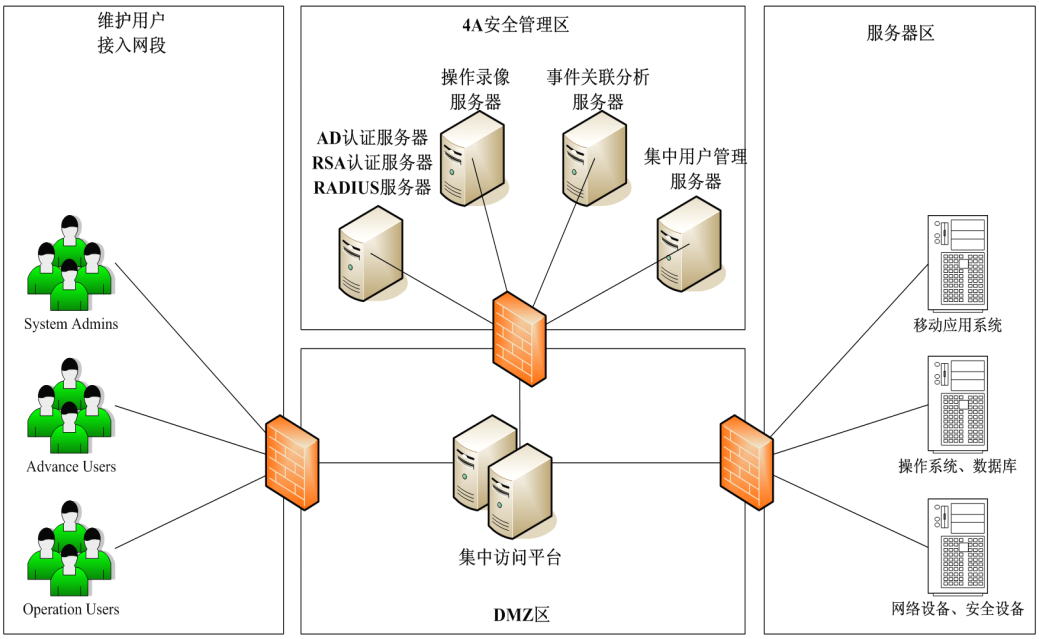



- 集中用户视图和应用视图
- 单一工具完成访问控制
- 用户流程化管理
- 自动化的用户信息/安全信息的管理
- 更容易使用新的安全技术
- 建立安全标准，具有高度可扩展性

# 第 2 章 IBM 身份管理与访问控制方案介绍

## 2.1 方案总体结构

IBM 身份管理与访问控制方案实现所有系统管理员对于所有管理对象的集中访问控制，同时提供用户单点登录、授权管理和用户行为审计的功能。如下图所示： IBM Tivoli 集中身份管理与访问控制平台方案的示意图：




解决方案以 IBM 集中访问平台为中心，集成了集中用户管理、集中用户认证、集中用户授权和集中用户审计的四个功能模块在内，共同组成完整的用户管理方案。各个模块的功能定义如下：

**(1) 集中用户管理**

用户管理服务器集中管理维护用户的主登录帐号与名下的各维护帐号。运维用户无须记住各个管理资源上的登录帐号和口令。

用户管理服务器定期自动更改所有后台服务器帐号口令。维护用户也可以进行自助服务，更改或重置个人的主登录帐号口令。

**(2) 集中用户认证**

维护用户凭个人的主登录帐号，登录个性化的集中访问平台。通过集中访问平台的单点登录服务，访问自己维护的各个系统，无须二次登录。集中访问平台与现有的 Windows AD 验证系统或RSA等强认证系统集成，实现集中认证功能。

**(3) 集中用户授权**

集中用户授权服务提供访问策略继承、组成员授权和基于角色的访问控制功能。一个用户完成身份认证、身份被确定以后，集中授权服务允许用户只能访问自己有权访问的信息，可以做哪些事情以及可以看到哪些信息。每次当用户试图访问一个资源时，将根据该资源的授权政策对用户的证书进行检查。

**(4) 集中用户审计**

集中用户事件审计服务器，集中记录用户在各个访问环节留下的访问日志，并进行关联整理和集中归档。保留原始事件日志的同时，建立维护用户的所有访问事件的关联事件日志。

## 2.2 方案功能模块描述

### 2.2.1 集中用户管理模块

在建立集中身份管理与访问控制平台时，用户身份的集中是一个必须的工作，否则就无法了解在不同应用中用户的对应情况是否一致。用户身份集中需要一个集中的用户身份管理系统，这个系统是所有应用、系统用户的管理点，由它来进行用户的同步，或者更新工作。同时，这个用户身份管理系统需要有一个用户管理的审批流程，这个流程和客户的管理规范相统一，从而保障整个用户管理的有序性，帮助管理层及时了解用户身份的变动情况。其目标在于：

- 通过目录服务，整合现有信息系统中现存、主流应用的用户管理数据库，使大量存在于不同数据库中的用户数据信息，统一于以目录为核心的统一用户管理平台之中，为安全有效的实施统一认证、授权管理平台、安全审计、单点登录等功能奠定坚实的基础；
- 通过LDAP目录服务，建立统一用户管理平台，实现分级模式的用户管理体系，强化对用户身份的管理；
- 通过目录服务，实现基于角色、粗粒度（基于URL）和细粒度（基于应用组件的方法调用）的访问策略管理，为企业建立规范的统一认证和授权管理支撑环境；
- 通过灵活、方便的委托管理机制，实现用户数据库的分级委托管理。为管理员提供统一的、基于Web的用户、角色和策略管理界面；
- 为用户提供自服务系统，用户通过自服务系统可以修改信息和口令。

IBM Tivoli集中用户管理模块，保证了所有用户帐号、访问资源和访问权限之间的正确关系。结构示意如下：通过该模块，集中管理用户的主登录帐号和后端被管理系统登录帐号的帐

号属性和口令，建立起账号申请及访问授权的工作流程。用户可以在自助管理网站上管理自己名下的所有帐号。如更改主登录帐号口令，批量更改系统帐号口令，提交帐号申请和权限申请等。

后端被管理系统上的用户帐号可以由用户自助修改，也可以由集中用户授权服务定期自动更改，所建立的用户帐号和口令可以自动同步到集中访问控制平台所使用的用户库中，运维用户籍助单点登录模块的功能，不必关注后台系统帐号。

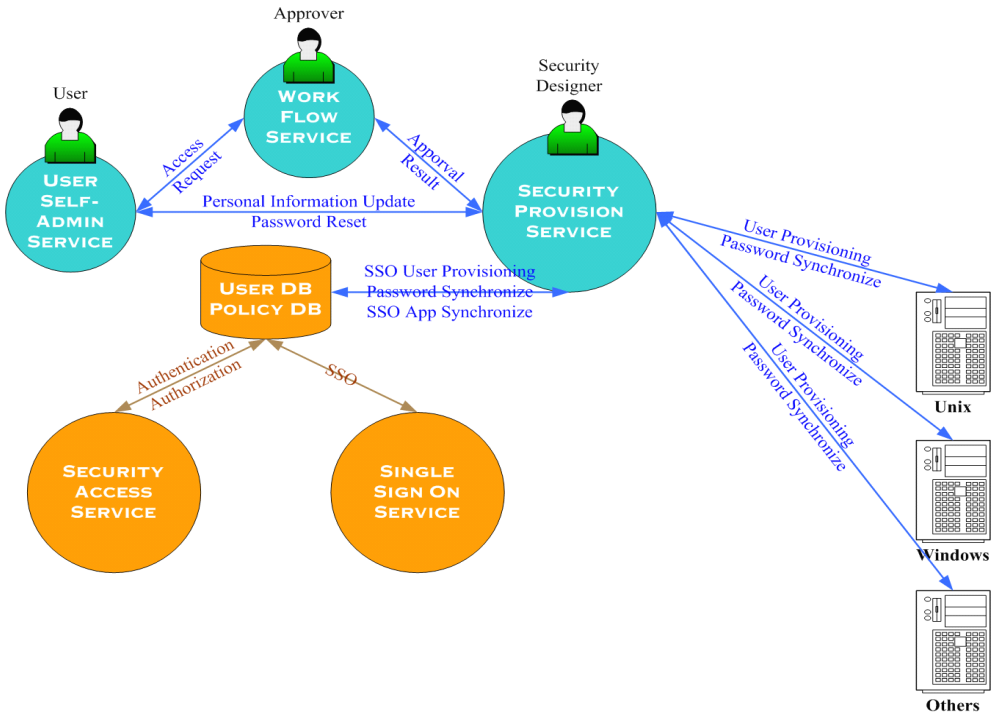



图3-1 集中用户管理

IBM推出了领先于业界的身份管理解决方案：IBM Tivoli Identity Manager，一套性能卓越、功能全面的身份管理系统，可以实现统一用户管理平台，包括用户的统一创建、维护、删除等功能。Tivoli Identity Manager将用户按照角色来管理，通过角色的定义可以将企业用户根据不同职位和职责进行分组，从而大大简化用户管理的负责度和降低管理成本。

Tivoli Identity Manager供一个功能全面的、图形化的工作流程及用户审批管理流程 (添加、修改、禁用、启用、删除)，很容易地把整个工作流程制作出来。此外，Tivoli Identity Manager 提供用户自助式服务功能；包括用户对个人信息的修改、个人账号密码的修改、密码提取等自助功能。

### 2.2.2集中用户认证与授权模块

对于一个企业来说，建立一个强健的、基于策略的安全身份认证和访问控制系统非常重要。一个完整的访问控制系统应该包括以下基本元素：身份验证，访问控制权限，审计，单点

登陆，高可靠性，整体结构的弹性和日志。

IBM Tivoli 集中用户访问模块，是运维用户身份管理与访问控制平台的“窗口”和“交通枢纽”，是用户访问后台资源的唯一途径。结构示意如下：用户利用浏览器，通过身份认证，登录集中访问控制平台，该平台对用户显示与其权限相对应的个性化访问页面，浏览器与访问控制平台之间采用HTTPS加密通讯，用户通过点击页面中相应的链接即可访问后端被管理的各类平台的目标服务器。用户只需完成一次主登录后，即可通过SSO模块直接登录其权限所允许访问的所有后端服务器。

集中访问平台完成用户的主登录，实现集中认证，认证机制支持多种类型，包括 RSA 验证和 RADIUS 验证等。

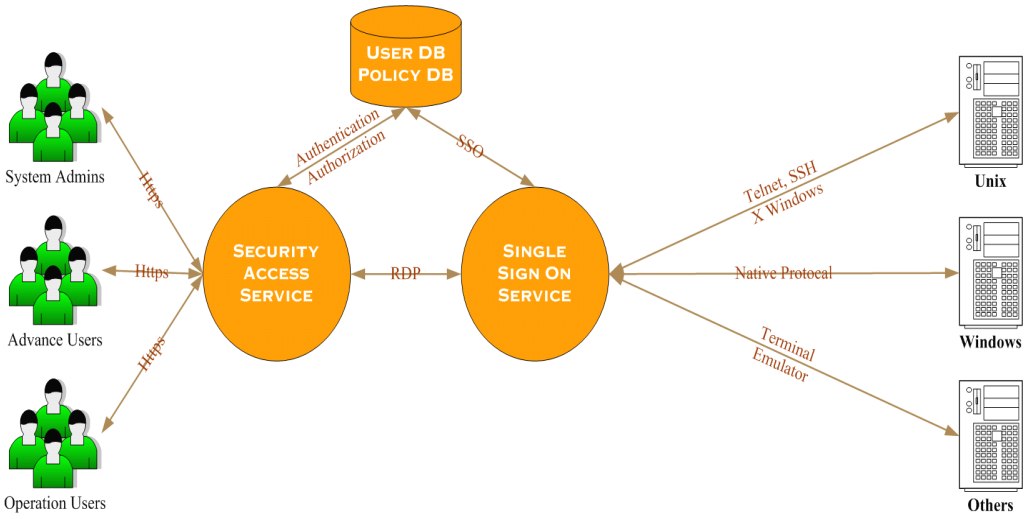



图3-2 用户集中访问和单点登录

IBM Tivoli Access Manager for e-Business可以提供高度可用的中央授权服务，使您能够更好地管理分散在各处的关键业务信息。透过IBM Tivoli Access Manager for e-Business提供安全授权和访问认证平台，管理用户对资源的访问，论提供全面的安全和管理策略定义。Tivoli Access Manager for e-Business支持用户分组，并给每组赋予不同的权限，同时支持动态规则的制定，如动态业务授权以及在需要的情况下使用外部数据为应用提供授权支持。

Tivoli Access Manager for e-Business提供用户能够方便的单点登录(SSO)到跨越多个站点或者域的基于Web的应用程序，从而帮助减少企业服务帮助台的电话量以及由许多个密码所带来的其他安全性问题。有了Tivoli Access Manager for e-Business的帮助，用户只需登录一次，他们的身份信息将会被创建，同时传递给后台应用程序，这个过程对用户来说是完全透明的。然后，用户就能访问所有已经被Tivoli Access Manager for e-Business安全域认证过的基于 Web 的资源和 Web 应用程序。

一个用户完成身份认证以后，Tivoli Access Manager for e-Business授权服务允许用户只

能访问自己有权访问的信息。授权服务维护中央资料库中的授权政策，该资料库中列出了受到保护的内部网中所有的资源以及与每一资源相关的策略模板（访问控制列表）。政策模板规定用户访问和操纵资源时必须满足的条件。每次当用户试图访问一个资源时，将根据该资源的授权政策对用户的证书进行检查。这一模型允许集中维护授权策略信息 — 而不是将这些信息传输到用户桌面上。Tivoli Access Manager for e-Business授权服务可以提供访问策略继承、组成员授权和基于角色的访问控制功能。为实现高可用性，可以对授权服务进行复制。

### 2.2.3集中用户审计模块

IBM Tivoli 集中用户审计模块，是运维用户身份管理与访问控制平台的“档案馆”，不仅真实记录了用户的操作行为和操作日志，并依据档案整理技术（关联分析），把分散的用户行为事件建立了关系索引，以便后期审计。

结构示意如下：事件关联分析模块提供集中操作审计，通过收集安全访问模块、SSO 模块、用户管理模块以及各个被管理系统上操作系统、数据库、应用、设备上的用户操作日志，来集中进行关联分析和归档。

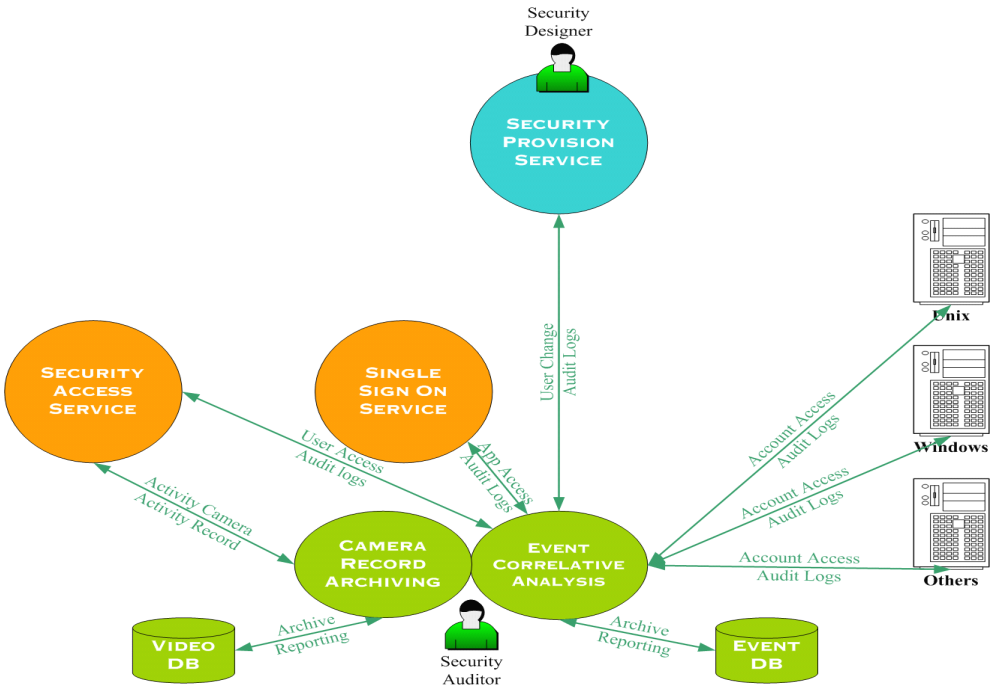


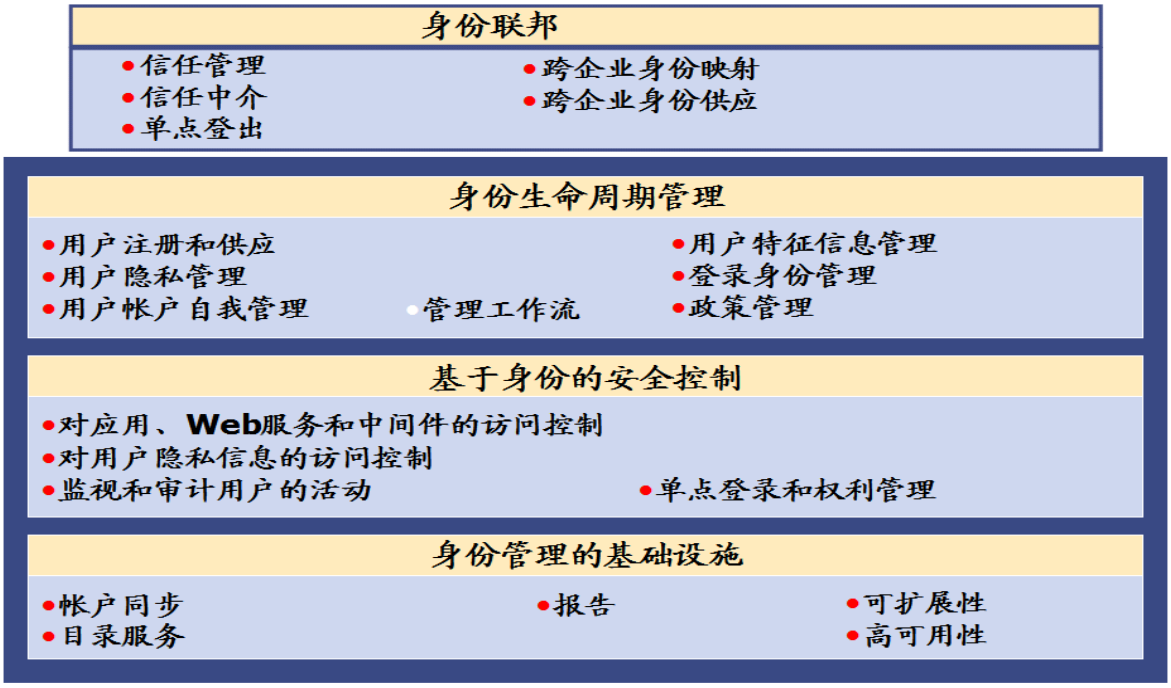

图3-3 集中日志审计

# 第 3 章 为什么选择 IBM 身份管理和访问控制解决方案

## 3.1 IBM 身份管理和访问控制方案优势

### 3.1.1 完整、集中、成熟的解决方案

IBM Tivoli 在用户身份管理和访问平台领域提供的是一个非常完成的解决方案。从 2004年开始，IBM就发布了身份管理蓝图以提供了一个全面的技术视图：




基于IBM 身份管理蓝图，IBM Tivoli 提供了包括目录服务、目录集成、身份管理、访问管理以及联邦身份管理等全面的解决方案。IBM Tivoli 安全产品得到业界的高度认证，都分布在 Gartner 权威产品评比象限的领先区域。

IBM Tivoli 的集中身份管理和统一访问认证解决方案具有相当的成熟性，在国内已经有7年多的客户使用经历(2002年第一个企业级部署)；客户分布在各个行业，从金融、电信，到制造业，从政府机关到中小企业，无处不在。曾经被客户用户管理面向全球的员工(COSOCN部署的集中身份管理和统一访问认证系统需要支持分布于全球的员工)；更是国内第一个真正的全国两级部署的集中身份管理和统一访问认证系统(系统部署于总部及三十一个省)；集成多种商业应用和客户自己的多个应用等。

### 3.1.2 高度扩展性的体系架构

作为业界使用最广泛的安全解决方案，Tivoli身份管理解决方案提供了高度扩展性的体系结构，从而可以满足电信企业的部署要求。

### 3.1.3强大的应用支持能力

作为企业的身份管理平台，Tivoli 解决方案可以支持为目前市场上主流的商业软件提供身份管理集成和认证集成，如SAP系统、SharePoint Portal Server、MS Exchange Server、Net环境以及自己开发的应用软件。

### 3.1.4独特的混合身份管理模式

业界唯有IBM Tivoli在身份生命周期管理上提供独特的混合身份管理模式，即同时提供基于角色的管理模式和基于请求的管理模式，这解决了困扰客户很久的身份管理模式的问题。

IBM作为全球领先的身份管理方案提供商，率先提出了请求管理模式和混合管理模式，从而提出了解决这一难题的方法。

### 3.1.5 基于策略的管理

对于身份管理而言，策略管理和策略检查是最为重要的部分。身份管理不仅需要策略管理，更需要策略检查。这主要是因为身份管理不是替换原有应用和系统的身份管理模块，而是一个集中的管理实现，所以帐户管理人员需要及时了解各个身份系统是否存在不符合策略的身份变化，如果没有这种能力，集中的帐户管理变成一纸空文。

Tivoli身份管理系统提供了全面的策略管理，其中就包括策略检查，定期对各个被管理的帐户资源进行策略扫描，从而发现不符合身份管理策略的帐户以便于及时处理，如挂起或者告警。同时，Tivoli身份管理系统提供对帐户策略修改给出模拟计算以便于帐户管理员了解帐户策略变化的影响，以及进行正确性校验。

## 3.2 丰富的大型项目实施管理经验和资深团队

### 3.2.1科学有效的项目管理方法和成熟的项目实施方法论。

IBM 公司在身份及访问管理领域内拥有丰富的项目实施经验，在这些项目的实施过程中，IBM 公司不断总结、形成并完善了自己的身份及访问管理项目实施方法论以及科学有效的项目管理方法。作为信息安全体系建设中具有一定特殊性的身份及访问管理领域，在项目的实施过程中，由于既涉及到管理领域，又涉及到与实际生产管理系统进行有效集成的技术领域，因此

有着与其他安全项目和管理项目不同的特点和要求，IBM 公司完全能够依托特有的科学有效的项目管理方法和成熟的项目实施方法论的基础上，对项目各阶段的实施工作进行有效的管理和资源的分配，从而确保本项目在地域分布广的情况下最终成功实施。

### 3.2.2 资深的项目实施顾问保证用户梳理工作的顺利完成

IBM 公司拥有大量的具有丰富经验的身份及访问管理项目实施经验的资深项目实施顾问，特别是在国内，拥有深刻理解国内用户在集中用户管理与统一认证方面的特殊需求的资深项目实施顾问。对于电信行业用户量大的特点，身份及访问管理项目所要面临的比较大的技术难题就是系统的稳定性和可用性，一定是只有经过大型集中用户管理项目的锻炼和考验，才能够快速、正确地完成这项工作。IBM 公司能够为本项目提供本地资深的项目实施顾问，从而确保本项目的最终成功实施。

### 3.2.3 成熟的产品和技术确保覆盖所有的应用系统要求

作为一个企业级集中用户管理与统一认证服务平台，所涉及的平台种类多，应用结构复杂，这就要求必须能够使用成熟的产品和技术来进行解决方案的涉及和实现，来保证能够覆盖最大范围及最多种类的系统平台，从而减少系统的开发量同时提供强大的系统可靠性。IBM 公司所提供的集中用户管理以及统一认证产品自发布以来，在全球拥有大量的大型企业用户，是一个完全成熟并且完全能够适应种类庞大的应用系统平台的产品。

# 第 4 章 IBM 中国公司简介

IBM，即国际商业机器公司，1911年创立于美国，是全球最大的信息技术和业务解决方案公司，业务遍及170多个国家和地区。2008年，IBM 公司的全球营业收入达到1036亿美元。

IBM 与中国的业务关系源远流长。早在1934年，IBM 公司就为北京协和医院安装了第一台商用处理机。随着中国改革开放的不断深入，IBM 在华业务日益扩大。80年代中后期，IBM 先后在北京、上海设立了办事处。到目前为止，IBM 在中国的办事机构进一步扩展至26个城市，从而进一步扩大了在华业务覆盖面。伴随着 IBM 在中国的发展，IBM中国员工队伍不断壮大，目前已达到14000人。除此之外，IBM 还成立了10 家合资和独资公司，分别负责制造、软件开发、服务和租赁的业务。 同时，IBM 非常注重对技术研发的投入。1995年，IBM 在中国成立了中国研究中心，是 IBM 全球八大研究中心之一，现有200多位中国的计算机专家和3000多位中国软件工程师专攻整合中间件，数据库，Linux 等领域的产品开发。

二十多年来，IBM 的各类信息系统已成为中国金融、电信、冶金、石化、交通、商品流通、政府和教育等许多重要业务领域中最可靠的信息技术手段。IBM 的客户遍及中国经济的各条战线。 与此同时，IBM 在多个重要领域占据着领先的市场份额，包括：服务器、存储、服务、软件等。

对于IBM在中国的出色表现和突出贡献，媒体给予了 IBM 十分的肯定。IBM 先后被评为“中国最受尊敬企业”、“中国最受尊敬的外商投资企业”、“中国最具有价值的品牌”、“中国最佳雇主”、“中国最受赞赏的公司”等。2005至2007年，IBM 连续三次被中国社会工作协会企业公民工作委员会授予“中国优秀企业公民”荣誉称号。

Tivoli 安全系列软件是业界领先的安全身份管理技术软件，是 IBM 信息安全软件的核心部分。IBM Tivoli是唯一一个跨越主机系统、客户机/服务器系统、工作组应用、企业网络、Internet服务器的端到端的解决方案。IBM 单在Tivoli Software分部就有超过2,000名安全员工。包含400多名安全开发人员及100多名安全支持人员。IBM每年投入多达1亿美元于安全方面的研发预算。 Tivoli 安全系列软件以 IBM 的世界级服务、支持和研究为坚强后盾，为客户提供一个无缝集成、灵活的随需应变基础架构管理解决方案，采用强健的安全机制将雇员、业务伙伴和客户连接起来。能够使企业降低身份管理和认证的总体管理成本，保障和实施信息安全观空，提高IT基础架构的管理及服务水平。

今年，IBM 中国公司将秉承“成就客户、创新为要、诚信负责”的核心价值观，在全球化的视野和布局下，努力成为中国客户的创新伙伴，为中国建设“创新型国家”尽一份心力。