通过添加安全性、灵活性和敏捷性来增强密码管理

IBM Redbooks 解决方案指南

员工日常必须管理的登录和密码数量一直以来都令员工头疼不已，并导致生产力下降。员工必须记住各种应用程序的登录信息。其中许多应用程序都要求使用不同的用户名和密码，具有不同的密码复杂性需求，并且在较短的时间间隔内强制更改密码。随着每个附加业务应用程序的部署，员工必须管理的登录次数也不断增加。企业帮助热线经常承受着为员工恢复丢失或者忘记的登录信息所带来的压力。这些因素结合在一起导致安全性风险提升，并增加了帮助热线的成本，罕有企业能够对其放任自流，不去处理。

通过使用 IBM® Security Access Manager for Enterprise Single Sign-On，您的组织可以集中受管的解决方案来应对这些严重的安全性、生产力与合规性挑战。图 1 显示了该解决方案的概述。

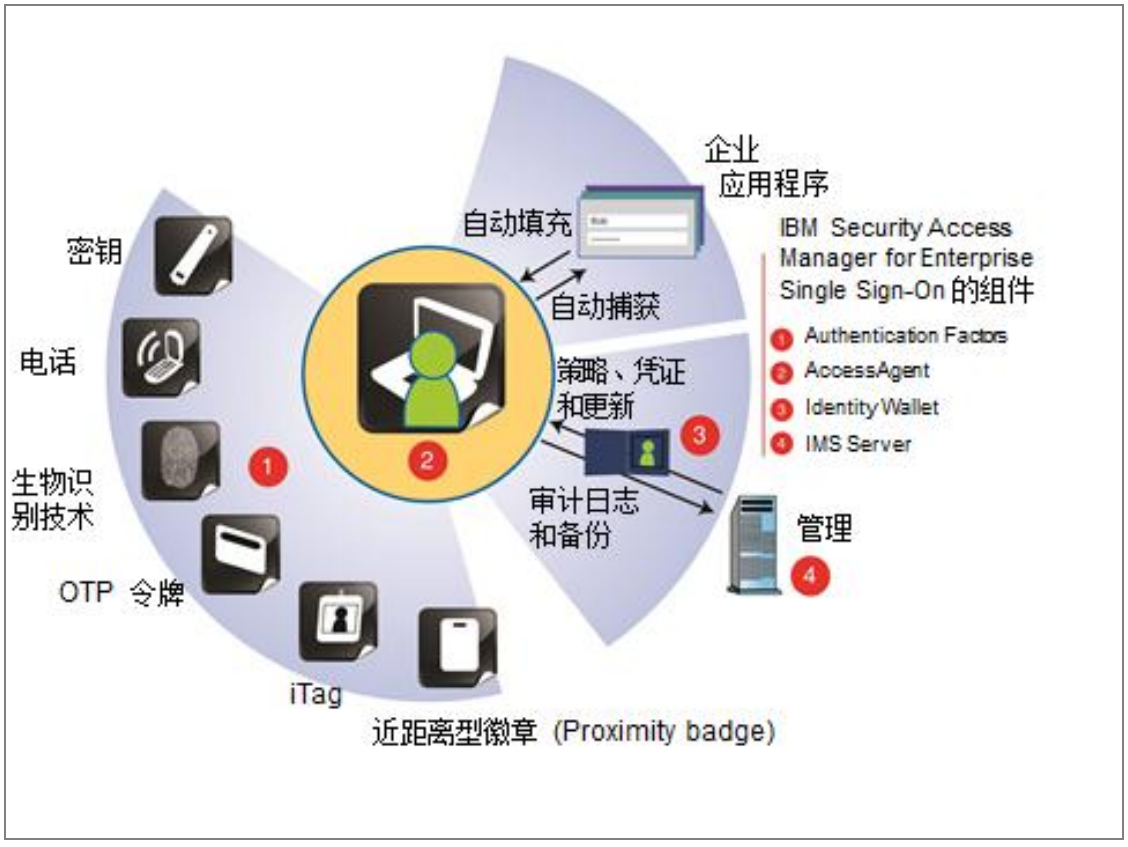

图 1. IBM Security Access Manager for Enterprise Single Sign-On 的概述

您知道吗？

用户经常抱怨必须记住多个密码，而计算机安全性中主要的安全漏洞就在于所选密码太弱。由于密码太弱或者密码管理不够安全所导致的安全违规随处可见。IBM Security Access Manager for Enterprise Single Sign-On 提供集中式解决方案，用于密码管理和自助服务，灵活且强大的认证机制并支持使用共享的虚拟工作站，而该解决方案也由此脱颖而出。

业务价值和解决方案概述

IBM Security Access Manager for Enterprise Single Sign-On 有助于您解决繁琐的密码难题。用户必须记住且只需记住一个密码，无需再为所有企业应用程序提供复杂的密码。用户只需通过一次认证，其余全部交由 IBM Security Access Manager for Enterprise Single Sign-On 处理。IBM Security Access Manager for Enterprise Single Sign-On 可提供以下主要业务价值：

- 以高度安全的方式管理密码

  IBM Security Access Manager for Enterprise Single Sign-On 可保护密码相关的应用程序和数据。它使用可用的最强密码术，包括高级加密标准 (AES) 和三重数据加密标准 (DES)。IBM Security Access Manager for Enterprise Single Sign-On 符合（美国）联邦信息处理标准（Federal Information Processing Standard，FIPS）140-2，旨在帮助金融机构、政府机构、医疗卫生机构和其他组织满足管控其运营的严格的隐私和安全法规。IBM Security Access Manager for Enterprise Single Sign-On 还可提供第二因子认证，以进一步增强安全性。它允许基于用户或机器混合并匹配各种不同的因子。如果这些因子存在，那么 IBM Security Access Manager for Enterprise Single Sign-On 可以对其加以使用。

- 降低帮助热线成本并改善员工生产力

  IBM Security Access Manager for Enterprise Single Sign-On 自助服务密码重置功能可以减少或者消除与忘记密码和由于帐户锁定导致丧失员工生产力相关的成本。忘记密码和由于失败尝试次数过多导致的帐户锁定会给企业帮助热线施加巨大压力。IBM Security Access Manager for Enterprise Single Sign-On 可提供可配置的功能，以便用户以满足各种安全性需求的方式来执行密码自助服务。可基于可配置的策略来定制和允许或禁止用户与密码更改、重置和帐户锁定及解锁功能进行交互的各种方式。IBM Security Access Manager for Enterprise Single Sign-On 使企业得以灵活决定将这些密码和帐户服务功能交由帮助热线和/或用户。密码重置功能提供了重置您的 IBM Security Access Manager for Enterprise Single Sign-On 密码以重新获取对您的桌面环境的访问权的功能。它不会重置任何特定于应用程序的密码。

- 通过审计和报告展示合规性

  IBM Security Access Manager for Enterprise Single Sign-On 在企业桌面上为细颗粒度的用户活动提供了内建的审计和报告功能。它可以记录审计事件，包括应用程序上用户的登录和注销。可通过定制审计机制来捕获与用户活动相关的其他信息。该产品随附多种包含的报告，但是由于所有审计数据均位于可查询的单一关系数据库中，因此可生成定制报告。

- 便于部署

  通过基于 Web 的管理控制台、高级目录集成和易于部署的客户端软件进行 IBM Security Access Manager for Enterprise Single Sign-On 的实施和管理。所有管理功能均从集中的 Web 管理控制台 (AccessAdmin) 来执行。AccessStudio 应用程序中的即点即选向导可以指导管理员完成概要文件配置的各种任务。管理员可以从具有可连接至服务器的 Web 浏览

器的任何位置访问 AccessAdmin 控制台。IBM Security Access Manager for Enterprise Single Sign-On 使用预先存在的用户存储库，无需修改目录模式或用户资源库的任何其他方面。

- 高性能

  在所有私有桌面环境、共享桌面环境和漫游桌面环境中，IBM Security Access Manager for Enterprise Single Sign-On 的速度都不打任何折扣。它在为用户提供对其应用程序的单点登录 (SSO) 体验时，仅使用最少的资源。由于其特定于事件的资源使用，IBM Security Access Manager for Enterprise Single Sign-On 对客户机和网络的影响都是最低限度的。无需额外的硬件或软件。

- 集成企业身份管理系统

  IBM Security Access Manager for Enterprise Single Sign-On Provisioning Bridge 通过自动执行凭证分发过程来扩展 IBM Security AccessManager for Enterprise Single Sign-On 生成的收益。IBM Security Access Manager for Enterprise Single Sign-On Provisioning Bridge 使用其 API 库来支持身份管理软件自动供应 IBM Security Access Manager for Enterprise Single Sign-On 用户凭证。通过这种方法，用户无需再知道其应用程序的用户名或密码，因为其用户名或密码可得到透明的管理。

  如果用户需要知晓某特定应用程序的用户名和密码，可以通过访问凭证库 (Wallet) 来获取此信息。仅当用户获得对 IBM Security Access Manager for Enterprise Single Sign-On 的认证之后才能进行此访问。如果用户在工作站中未使用 AccessAgent，那么可以通过使用 AccessAssistant 基于 Web 浏览器的界面来访问此信息。即使未集成身份管理软件，IBM Security Access Manager for Enterprise Single Sign-On 仍通过这些组件提供高度可用且安全的密码显示过程。

- 为多媒体终端机器和虚拟桌面提供 SSO

  不幸的是，允许他人共享工作站的便利仍然存在风险。用户经常离开多媒体终端机器而忘记注销，这样可能会暴露敏感数据。IBM Security Access Manager for Enterprise Single Sign-On 通过自动执行不活动会话和应用程序关闭的功能来应对此威胁。自动化包含各种功能部件，例如通过射频识别 (RFID) 近距离型密钥或智能卡拔出来进行自动走开注销等。

  IBM Security Access Manager for Enterprise Single Sign-On 为漫游桌面实施提供健全的会话管理支持。它使用各种技术（例如，Microsoft Windows Terminal Services 和 Citrix XenApps）以及共享桌面或多媒体终端机器和专用桌面。用户可以在各工作站之间轻松、安全地进行漫游。IBM Security Access Manager for Enterprise Single Sign-On 还包含对于保护虚拟桌面基础结构 (VDI) 技术（例如，VMware View）的支持。此外，IBM Security Access Manager for Enterprise Single Sign-On 包含通过漫游桌面方式和通过 Web Workplace 进行的瘦客户机和无客户机访问。

解决方案体系结构

IBM Security Access Manager for Enterprise Single Sign-On 引入了一个层来对用户进行一次认证，然后自动检测并处理用户凭证的后续请求，由此提供其 SSO 功能。

IBM Security Access Manager for Enterprise Single Sign-On 可分为以下体系结构组件，如图 1 中所示：

- Authentication Factors

  IBM Security Access Manager for Enterprise Single Sign-On 支持各种认证因子以对用户进行认证。除基于用户名和密码的标准认证之外，可按近距离型徽章或构建徽章来对用户进行认证。例如，主动或被动 RFID、指纹、短消息服务 (SMS) 提供的一次性密码 (OTP) 或 OTP 令牌，或者 USB 令牌。

- AccessAgent

  AccessAgent 在每一个 Windows 桌面端点、Windows Server Terminal Services 会话、VMware vSphere 虚拟桌面界面会话和 Citrix XenApp Presentation Server 会话上运行。AccessAgent 负责对用户进行认证。它可在 Windows 中以及 AccessProfiles 内定义的应用程序集中自动执行 SSO。AccessAgent 可扩展 Windows Graphical Identification and Authentication (GINA) 动态链接库 (DLL) 链，为自助服务或强认证提供额外的功能。

- Identity Wallet

  Identity Wallet（又称为 Wallet）保留 SSO 所需的用户凭证。在用户认证成功后，它会从 IBM IMS™ Server 装入 AccessAgent，因此，即使端点从计算机网络断开连接，凭证仍可用。为保护凭证避免遭到篡改或失窃，Identity Wallet 以强大的加密机制进行加密。

- IMS Server

  IMS Server 是用户数据、AccessProfiles、Identity Wallets 和机器概要文件的集中存储库。IMS Server 可提供基于 Web 的界面，用于管理用户和策略。

使用方案

在此使用方案中，某医疗卫生供应商运营着多家独立诊所，每家诊所各自占有一栋建筑并提供预防护理、心脏手术和门诊服务。该医疗卫生供应商拥有大量医护人员和支持人员，这些人员直接受雇于该公司，另有小部分与公司签订合同的独立外科医生。

该医疗卫生供应商维护着财务数据和私人客户数据（患者、研究伙伴和附属医院）。大部分记录以电子形式保存在 SAP 系统中。此外，公司所有员工均可使用电子邮件进行内部通信以及与外界（患者和外部伙伴）进行通信。

图 2 显示了该医疗卫生公司的体系结构图，其中包含单独的网络区域之间的主要通信线路。

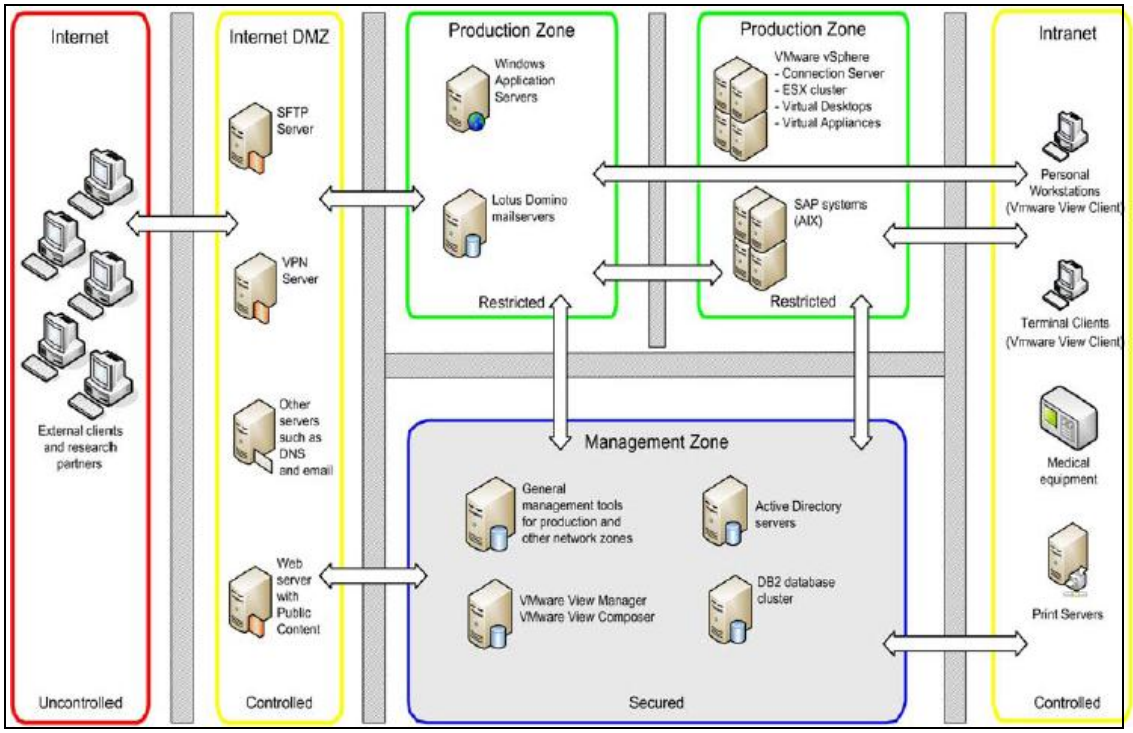

图 2. 该医疗卫生公司当前的体系结构概述

该医疗卫生公司希望实现以下短期业务目标：

- 通过交付卓越的个人医疗卫生体验来改善患者护理的质量和可用性以及满意度。
- 增加对所有患者相关信息的保护，并应对合规性需求、新兴技术和数据爆炸所带来的多样化的安全性风险。
- 促进对于数据隐私法律和行业标准（例如，健康保险可移植性和责任法案 (HIPAA) 和支付卡行业数据安全标准 (PCI-DSS)）的总体合规性的管理和展示。

总而言之，该医疗卫生公司希望获得成熟的安全性解决方案，以预防信息泄露并确保认证的可信任性，以及影响患者的所有行动的个别可跟踪性和可计帐性。

作为 IBM Security Access Manager for Enterprise Single Sign-On 的基本级别实施，以下组件得到了部署：

- 集中用户资源库或目录

  集中用户资源库可以是多种受支持的存储库之一，包括 Active Directory、Novell 和一般轻量级目录访问协议 (LDAP)。在安装任何 IBM Security Access Manager for Enterprise Single Sign-On 组件之前，集中用户资源库必须已就位。在该医疗卫生公司环境中，集中用户资源库为 Active Directory，如图 2 所示。

- IMS Server

  IMS Server 是基于 Java 的应用程序，在其自己的 IBM WebSphere® Application Server 实例上运行。它可以是 Windows 服务器平台上的软件安装，或者也可以集成到预封装的虚拟设备中。IMS Server 在 Management Zone 中部署，如图 2 所示。

- IMS 数据库

  IMS 数据库可存储 IBM Security Access Manager for Enterprise Single Sign-On 的所有配置、策略和用户数据。该数据库可在现有数据库服务器上创建，或者也可以安装在 IMS Server 所在的同一系统上。受支持的数据库包括 IBM DB2®、Microsoft SQL 和 Oracle。在该医疗卫生公司环境中，使用现有的 DB2 数据库作为数据库，如图 2 中所示。

- AccessAgent

  AccessAgent 安装在由 IBM Security Access Manager for Enterprise Single Sign-On 管理的每个客户机系统、Windows Terminal Server、VMware Virtual Desktop 和 Citrix XenApp 服务器上。

- AccessStudio

  AccessStudio 是用于创建 AccessProfiles 的管理工具。它只能安装在一个工作站上，通常安装在一个或多个 IMS Server 管理员的工作站上。由于 AccessStudio 需要 AccessAgent，安装 AccessStudio 之前，必须将 AccessAgent 安装在要安装 AccessStudio 的同一工作站上。

部署基本基础结构组件之后，该医疗卫生供应商实施了以下功能：

- 密码自助服务

  如果该医疗卫生公司内的用户忘记其 Microsoft Windows 密码，那么必须联系 IT 支持热线，由支持热线人员在执行必要的安全检查之后代表其重置密码。IBM Security Access Manager for Enterprise Single Sign-On 通过提供产品的密码自助服务功能来克服此问题。与 IMS Server 连接的用户可以自行重置其密码。

  通过使用 IBM Security Access Manager for Enterprise Single Sign-On 的密码自助服务功能部件，用户可以基于挑战响应流程从任何工作站重置其主要认证。（主要认证可以是 IBM Security Access Manager for Enterprise Single Sign-On 密码或桌面密码。）所有问题均可定制且可配置。当已配置 IBM Security Access Manager for Enterprise Single Sign-On 密码自助服务（无需安装其他组件）时，用户无需呼叫技术支持。不仅如此，用户无需等待管理员来重置密码。用户可以提供在 AccessAgent 登录阶段设置的辅助密钥。无需安装其他组件即可使用密码自助服务功能。

- 使用 RFID 的强认证

  该医疗卫生公司希望为其医疗员工提供安全的*快速用户切换*方式。这些使用遍布于所有医院的共享终端客户机的用户需要更快速且更方便的方式来登录系统。医疗员工经常需要以简短的注释来更新患者记录，然后再诊疗下一位患者，但是他们每天都需要频繁输入简短的注释。同时，医疗员工还需要每天多次输入其用户名和（复杂的）密码来访问其虚拟桌面环境，这容易造成不满。该公司致力于解决此问题。但是，它不愿意牺牲安全性。

  该医疗卫生公司选择对所有共享终端客户机部署 RFID 徽章阅读器。通过使用该功能，医疗员工可以将其 RFID 访问徽章链接到其 SSO 用户名和密码。该策略旨在提示医疗员工每天提供一次其 RFID 徽章和密码。对于其轮班的其余时间，员工可以将 RFID 徽章提供给阅读器，即可自动登录至其 SSO Wallet。

- 漫游桌面实施

  当某个用户在半公开区域通过使用密码或 RFID 徽章登录共享工作站时，会自动启动到该用户的虚拟桌面的连接。用户登录此虚拟桌面的过程必须通过安全且防篡改的方式发生。

  登录虚拟桌面的用户必须能够在不提供认证凭证的情况下使用受支持的应用程序。此功能的工作方式必须与这些应用程序在所连接的共享工作站上运行时无异。当用户从共享工作站注销时，漫游虚拟桌面及其应用程序必须继续在虚拟基础结构上运行。共享工作站不活动策略必须尽可能严格才能预防他人访问停留中的虚拟桌面会话。不活动会话需要自动终止。

  医护员工使用分布式工作站，通过使用其 RFID 徽章自动登录并连接至 VMware ESXi Server 上托管的虚拟桌面。图 3 显示了目标解决方案组件体系结构。

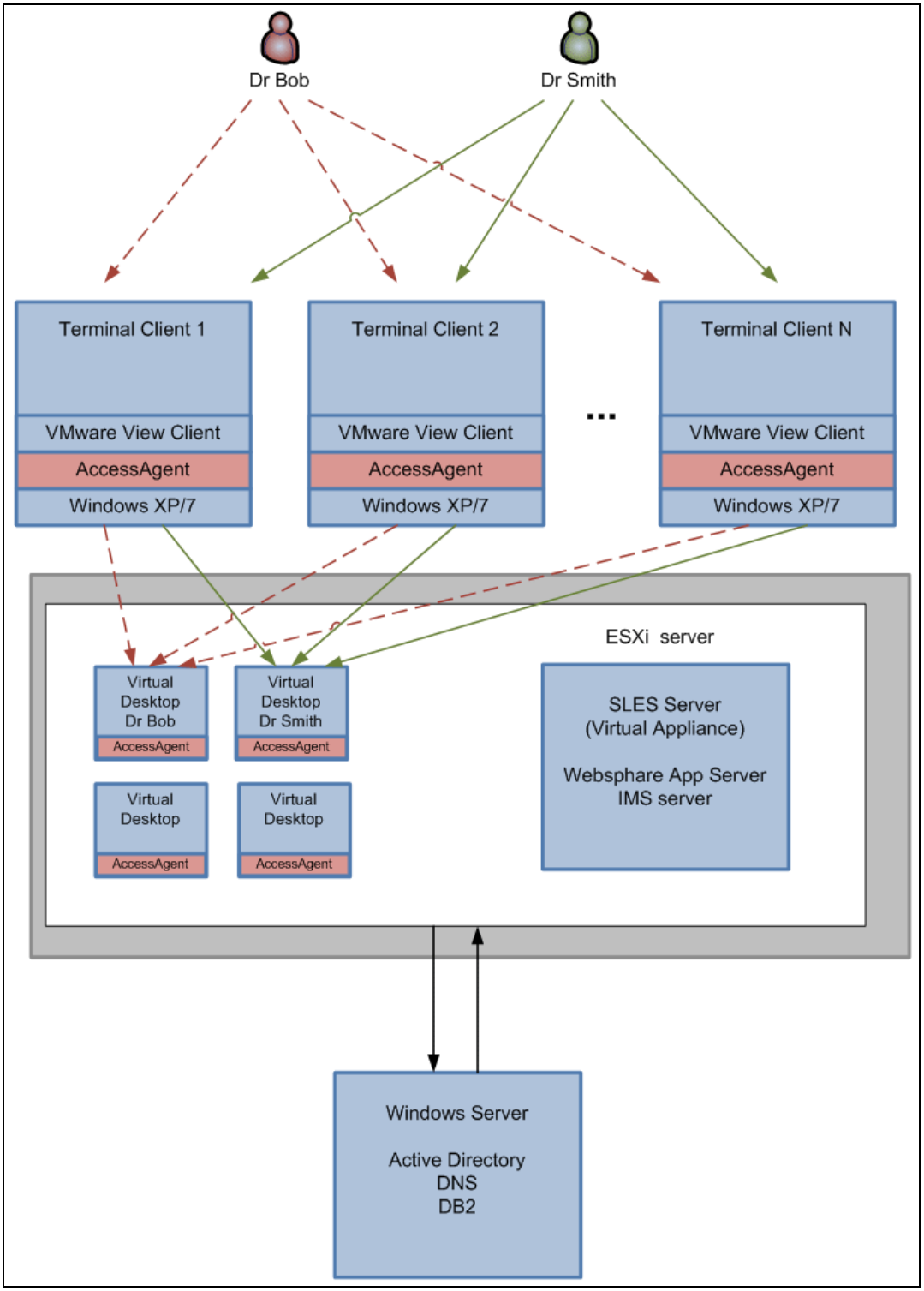
Dr Bob
Dr Smith
Terminal Client 1
VMware View Client
AccessAgent
Windows XP/7
Terminal Client 2
VMware View Client
AccessAgent
Windows XP/7
...
Terminal Client N
VMware View Client
AccessAgent
Windows XP/7
ESXi server
Virtual Desktop Dr Bob
AccessAgent
Virtual Desktop Dr Smith
AccessAgent
Virtual Desktop
AccessAgent
Virtual Desktop
AccessAgent
SLES Server
(Virtual Appliance)
Websphare App Server
IMS server
Windows Server
Active Directory
DNS
DB2

图 3. 漫游桌面体系结构

订购信息

本产品仅可通过 IBM Passport Advantage® 获取。它不可作为用收缩性薄膜包装的产品提供。在 IBM 公告函（请参阅“相关信息”部分）中提供了详细的订购信息。

相关信息

要了解更多信息，请参阅以下文档：

- *Enterprise Single Sign-On Design Guide Using IBM Security Access Manager for Enterprise Single Sign-On 8.2*，SG24-7350
  http://www.redbooks.ibm.com/abstracts/sg247350.html?Open

- *BIO-key Biometric Service Provider for IBM Security Access Manager for Enterprise Single Sign-On*，REDP-4892
  http://www.redbooks.ibm.com/abstracts/redp4892.html?Open

- *A Guide to Authentication Services in IBM Security Access Manager for Enterprise Single Sign-On*，REDP-4835
  http://www.redbooks.ibm.com/abstracts/redp4835.html?Open

- *A Guide to Writing Advanced Access Profiles for IBM Tivoli Access Manager for Enterprise Single Sign-On*，REDP-4767
  http://www.redbooks.ibm.com/abstracts/redp4767.html?Open

- *Setup and Configuration for IBM Tivoli Access Manager for Enterprise Single Sign-On 8.1 for Single-Server and Cluster Environments*，REDP-4700
  http://www.redbooks.ibm.com/abstracts/redp4700.html?Open

- IBM Security Access Manager for Enterprise Single Sign-On 产品页面
  http://www.ibm.com/software/tivoli/products/access-mgr-esso

- IBM 公告函和销售手册
  http://www.ibm.com/common/ssi/index.wss?request_locale=en

  在该页面上，输入 IBM Security Access Manager for Enterprise Single Sign-On，然后单击 **Search**。在下一个页面上，按信息类型、地理位置、语言或者这三种选项的组合来缩小您的搜索结果范围。

声明

本信息是为在美国提供的产品和服务编写的。

IBM 可能在其他国家或地区不提供本文档中讨论的产品、服务或功能特性。有关您当前所在区域的产品和服务的信息，请向您当地的 IBM 代表咨询。任何对 IBM 产品、程序或服务的引用并非意在明示或暗示只能使用 IBM 的产品、程序或服务。只要不侵犯 IBM 的知识产权，任何同等功能的产品、程序或服务，都可以代替 IBM 产品、程序或服务。但是，评估和验证任何非 IBM 产品、程序或服务，则由用户自行负责。IBM 公司可能已拥有或正在申请与本文档内容有关的各项专利。提供本文档并未授予用户使用这些专利的任何许可。您可以用书面方式将许可查询寄往：

IBM Director of Licensing, IBM Corporation, North Castle Drive, Armonk, NY 10504-1785 U.S.A.

本条款不适用英国或任何这样的条款与当地法律不一致的国家或地区：INTERNATIONAL BUSINESS MACHINES CORPORATION“按现状”提供本出版物，不附有任何种类的（无论是明示的还是暗含的）保证，包括但不限于暗含的有关非侵权、适销和适用于某种特定用途的保证。某些国家或地区在某些交易中不允许免除明示或暗含的保证。因此本条款可能不适用于您。本信息中可能包含技术方面不够准确的地方或印刷错误。此处的信息将定期更改；这些更改将编入本资料的新版本中。IBM 可以随时对本资料中描述的产品和/或程序进行改进和/或更改，而不另行通知。

本信息中对非 IBM Web 站点的任何引用都只是为了方便起见才提供的，不以任何方式充当对那些 Web 站点的保证。那些 Web 站点中的资料不是 IBM 产品资料的一部分，使用那些 Web 站点带来的风险将由您自行承担。IBM 可以按它认为适当的任何方式使用或分发您所提供的任何信息而无须对您承担任何责任。涉及非 IBM 产品的信息可从这些产品的供应商、其出版说明或其他可公开获得的资料中获取。IBM 没有对这些产品进行测试，也无法确认其性能的精确性、兼容性或任何其他关于非 IBM 产品的声明。有关非 IBM 产品性能的问题应当向这些产品的供应商提出。本信息包含在日常业务操作中使用的数据和报告的示例。为了尽可能完整地说明这些示例，示例中可能会包括个人、公司、品牌和产品的名称。所有这些名字都是虚构的，若现实生活中实际业务企业使用的名字和地址与此相似，纯属巧合。

此处包含的任何性能数据都是在受控环境中测得的。因此，在其他操作环境中获得的数据可能会有明显的不同。有些测量可能是在开发级的系统上进行的，因此不保证与一般可用系统上进行的测量结果相同。此外，有些测量是通过推算而估计的，实际结果可能会有所不同。本文档的用户应当验证其特定环境的适用数据。

版权许可：

本信息包括源语言形式的样本应用程序，这些样本说明不同操作平台上的编程方法。如果是为按照在编写样本程序的操作平台上的应用程序编程接口（API）进行应用程序的开发、使用、经销或分发为目的，您可以任何形式对这些样本程序进行复制、修改、分发，而无须向 IBM 付费。这些示例并未在所有条件下作全面测试。因此，IBM 不能担保或暗示这些程序的可靠性、可维护性或功能。

本文档于 2012 年 12 月 7 日创建或更新。

请通过以下任一方式将您的意见发送给我们：

- 使用位于以下地址的在线**联系我们**审阅表单：
  ibm.com/redbooks
- 通过电子邮件将您的意见发送至：
  redbook@us.ibm.com
- 将您的意见邮寄至：
  IBM Corporation, International Technical Support Organization
  Dept. HYTD Mail Station P099
  2455 South Road
  Poughkeepsie, NY 12601-5400 U.S.A.

本文档可通过以下地址在线访问：**ibm.com**/redbooks/abstracts/tips0943.html

商标