Windows Server 2012 R2

Windows Server 2012 R2
访问与信息保护

用户

- 希望自行选择设备
- 希望能随时随地连接

IT

- 支持自带设备的同时维持合规性并保护数据

实际情况

- 全球智能可联网设备出货总量于 2012 年达到 12 亿部，2016 年将增长至 20 亿部。1
- 根据 Forrester 2012 年的一份报告，企业已将移动设备与应用安全列为首要任务，46% 企业认为未来 12 个月内改善或实施移动设备安全保护是“高”优先任务。另外 22% 企业认为这种做法“至关重要”。2
- 只有 30% 的公司针对员工个人拥有的智能手机具备相应的策略与工具；15% 完全不具备相关策略。3

1. IDC 新闻稿，IDC 预计到 2016 年，智能可联网设备出货量将增长 14%，其中大部分是平板与智能手机 (2012 年 9 月 26 日)

2. 企业移动设备行动倡议与规划基准，Forrester Research, Inc.，2012 年 10 月 10 日

3. 移动员工使用个人应用解决客户的问题 " 准备好了吗，是否愿意并能提供帮助？ "Forrester Consulting 于 2012 年 9 月受 Unisys 委托进行的一次调查

挑战

- 用户希望随时随地，用任何设备访问企业服务并获得一致的体验。
- 企业希望高效率管理各种消费类设备，同时在不影响数据安全的情况下继续提供高效率运维。

Windows Server 2012 R2 的解决方案

- 对非受管及自带设备简化注册与登记流程
- 需要时自动连接到内部资源
- 在多种设备上通过一致的方式访问公司资源
- 使用通用的身份访问内部环境与云端的资源
- 企业信息集中化，满足合规性与数据保护要求
- 对应用程序与数据实施基于策略的访问控制

访问与信息保护

Windows Server 2012 R2 访问与信息保护解决方案能让您的用户在几乎任何位置安全地访问企业资源，用自己惯用的设备维持生产力。通过充分利用现有的 Active Directory 投资并将其连接到 Windows Azure Active Directory，Windows Server 2012 R2 为 IT 提供了将用户身份与 Windows Azure 及其他云端身份技术结合在一起的能力。用户可以使用通用身份访问内部环境与云端的资源，一次登录即可访问所有应用程序与数据。

Windows Server 2012 R2 还提供了一套在 Active Directory 中注册自带非受管设备的机制，这样 IT 就会获知设备的存在，并将其考虑到访问策略中，随后用户即可访问企业资源。用户还可以使用 Windows Intune 管理服务登记自己的设备，并使用公司门户在访问应用程序、数据，以及自助服务设备管理时获得一致的体验。Windows Server 2012 R2 远程访问功能配合 Windows 8.1 可在需要时自动创建 VPN 连接并连接到内部资源。此外用户可以使用文件服务器角色新增的工作文件夹这一同步功能跨越设备访问自己的工作文档。

为了保护企业数据，Windows Server 2012 R2 可以让 IT 将企业信息集中保存，满足合规性与数据保护要求。将数据从笔记本等非受管的分散位置移动到受管位置，并将数据同步到设备，即可实现双重目标，让 IT 充分控制信息，用户则可按照喜欢的方式工作。基于策略的访问控制机制可用于应用程序与数据，该功能可充分考虑用户的身份，例如用户设备是否“已知”（已注册），并可考虑用户的位置（企业环境的内部或外部）。

无论您是大企业、服务供应商或中小企业，Windows Server 2012 R2 都能帮您对业务进行优化。

Microsoft

改进用户体验

Windows Server 远程访问	无需发起 VPN 连接，使用 DirectAccess 功能帮助用户远程工作，保持与企业网络的连接。如果用户启动的应用程序需要访问企业资源，Remote Access 还可自动发起 VPN 连接。
Web 应用程序代理	帮助 IT 部门根据所感知的设备及用户身份发布资源访问方式。通过与 AD FS 集成，IT 还可预先对用户与设备进行身份验证，并强制实施访问策略，例如要求设备必须注册或实施多因素身份验证。
加入工作空间	让 IT 部门了解非受管与自带的设备；实现企业数据访问的单点登录；将证书推送给设备，并在 Active Directory 中记录新设备的注册。
工作文件夹	帮助用户用安全的方式将数据从企业文件服务器同步到所有客户端设备（反之亦然）；确保数据总有一个副本保存在企业环境中，始终可用，可备份，并可通过动态访问控制与权限管理功能应用业务规则。
设备登记	通过 Windows Intune 将设备配置为可管理状态。随后用户即可使用公司门户轻松访问企业应用程序。
Windows Azure 移动服务	帮助开发人员集成并改进自己的应用程序，通过多项功能加快开发进程的速度，例如链接到数据源，身份验证，以及配置推送通知。
增强的 Active Directory 联合身份验证服务	提供增强的自带设备支持，包括消费类设备的注册服务，借此提供更可靠的访问、设备身份验证、敏感访问，及现代化的 LOB 应用。

混合式身份管理

身份管理	利用 Active Directory 联合身份验证服务连接到 Windows Azure，获得一致的云端身份。用户可充分利用通用身份，使用 Windows Azure Active Directory 帐户访问 Windows Azure、Office 365 及第三方应用程序。
虚拟化支持	帮助 IT 在更大规模环境下运行 Active Directory，通过域控制器克隆支持虚拟化与快速部署。

保护您的数据

多因素身份验证	利用与 Windows Azure 多因素身份验证的集成帮助 IT 在用户连接时强制实施多因素身份验证。
动态访问控制	根据内容对数据进行自动化识别与分类。与 Active Directory 权限管理服务的集成可自动加密文档。此外 IT 可针对多台文件服务器应用集中的访问与审计策略，并可用近乎实时的方式分类并处理新增和修改的文档。
选择性擦除	一旦设备丢失、被盗，或者需要退役，可擦除设备中的企业数据。

更多信息

下载并试用 Windows Server 2012 R2：
http://www.microsoft.com/zh-cn/server-cloud/products/windows-server-2012-r2

详细了解访问与信息保护解决方案：
http://www.microsoft.com/zh-cn/server-cloud/solutions/access-information-protection.aspx

Microsoft